

ETSI TR 103 954 V1.1.1 (2024-07)



TECHNICAL REPORT

**Cyber Security (CYBER);
Critical Security Controls for Effective Cyber Defence;
Mobile Communications Sector**

Reference

DTR/CYBER-00108

Keywordscyber-defence, cybersecurity, information
assurance, mobile**ETSI**650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<https://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary	4
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Applying the Critical Security Controls for effective risk control and enhanced resilience of the mobile communications sector.....	9
4.1 Introduction, Methodology and Use.....	9
4.2 Applicability Overview	12
4.3 Applying the Critical Security Controls and Safeguards.....	13
4.3.1 CONTROL 01 Inventory and Control of Enterprise Assets	13
4.3.2 CONTROL 02 Inventory and Control of Software Assets	16
4.3.3 CONTROL 03 Data Protection.....	19
4.3.4 CONTROL 04 Secure Configuration of Enterprise Assets and Software	23
4.3.5 CONTROL 05 Account Management	26
4.3.6 CONTROL 06 Access Management Control	28
4.3.7 CONTROL 07 Continuous Vulnerability Management	31
4.3.8 CONTROL 08 Audit Log Management	34
4.3.9 CONTROL 09 Email and Web Browser Protections	36
4.3.10 CONTROL 10 Malware Defences.....	38
4.3.11 CONTROL 11 Data Recovery.....	41
4.3.12 CONTROL 12 Network Infrastructure Management	43
4.3.13 CONTROL 13 Network Monitoring and Defence.....	45
4.3.14 CONTROL 14 Security Awareness and Skills Training	47
4.3.15 CONTROL 15 Service Provider Management	49
4.3.16 CONTROL 16 Application Software Security	51
4.3.17 CONTROL 17 Incident Response Management.....	54
4.3.18 CONTROL 18 Penetration Testing	56
5 GSMA Security Controls	58
5.1 GSMA Baseline Security Controls.....	58
5.2 Critical Security Controls Mapping to GSMA Baseline Security Controls.....	59
Annex A: Reverse Mapping of GSMA FS.31 Controls to ETSI Critical Security Controls	69
Annex B: Bibliography	74
History	75

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

Mobile communication networks, devices, and applications have become pervasive worldwide as a critical infrastructure for providing ICT services and applications. The protection of this infrastructure from cybersecurity threats by instituting effective risk control and enhanced resilience has received the global attention of governmental authorities and industry organizations ([i.1] through [i.9]). The present document addresses this protection challenge by providing guidance on individually applying the most current version of the Critical Security Controls for effective cyber defence to mobile infrastructure, especially individual user devices and applications ([i.12] and [i.13]). For compliance purposes, the Critical Security Controls have mappings to almost every known government and industry cyber security framework with extensive implementations for diverse operating systems and applications. Included in the present document is a mapping to the GSMA Security Controls framework together with summary of those Controls.

Introduction

The Critical Security Controls are a prioritized set of actions that collectively form a defence-in-depth set of best practices that mitigate the most common attacks against systems and networks. Under the auspices of the Center for Internet Security (CIS), the Controls are developed by a community of Information Technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the Controls come from a wide range of sectors including, retail, manufacturing, healthcare, education, government, defence, and others. While the Controls address the general practices that most enterprises should take to secure their systems, some operational environments may present unique requirements not addressed by the Controls.

The Controls started as a grassroots activity to identify the most common and important real-world cyber-attacks that affect enterprises every day, translate that knowledge and experience into positive, constructive action for defenders, and share that information to help enterprises focus their attention on the most fundamental steps they should take to defend themselves. As the Controls continue to be refined and re-worked through the expert community, the need for Controls guidance for the mobile communications sector became clear.

1 Scope

The present document applies the latest version of the Critical Security Controls ([i.10] and [i.15]) for effective risk control and enhanced resilience of the Mobile Communications sector and includes mappings to latest version of the GSMA Security Controls.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] [Directive \(EU\) 2022/2555](#) of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance).
- [i.2] [2020/0266 \(COD\), COM\(2020\) 595 final](#): "Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014".
- [i.3] [Directive \(EU\) 2022/2557](#) of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance).
- [i.4] [Regulation \(EU\) 2019/881](#) of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).
- [i.5] [Council Directive 2008/114/EC](#) of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance).
- [i.6] [Regulation \(EU\) 2022/2065](#) of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).
- [i.7] [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).
- [i.8] [COM\(2016\) 176 final](#): "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ICT Standardisation priorities for the digital single market".

- [i.9] [COM\(2020\) 67 final](#): "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Shaping Europe's digital future".
- [i.10] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".
- [i.11] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".
- [i.12] ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement".
- [i.13] ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".
- [i.14] GSMA: "[FS.31 Baseline Security Controls, Version 3.0](#)".
- [i.15] Center for Internet Security: "[Critical Security Controls Mobile Companion Guide, V8](#)".
- [i.16] Center for Internet Security: "[Critical Security Controls Version 8 Mapping to GSMA FS.31 Baseline Security Controls v3.0](#)".
- [i.17] [NIST Special Publication \(SP\) 800-53 Revision 5](#): "Security and Privacy Controls for Information Systems and Organizations".
- [i.18] Cloud Security Alliance, Mobile Working Group: "[Security Guidance for Critical Areas of Mobile Computing](#)".
- [i.19] [NIST Special Publication 800-124, Revision 2](#): "Guidelines for Managing the Security of Mobile Devices in the Enterprise".
- [i.20] FIRST: "[Common Vulnerability Scoring System version 4.0](#)".
- [i.21] [NIST Special Publication SP 800-163, Revision 1](#): "Vetting the Security of Mobile Applications".
- [i.22] NIST: "[Framework for Improving Critical Infrastructure Cybersecurity](#)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

2FA	Two-Factor Authentication
AAA	Authentication, Authorization, and Auditing
AD	Application Data
ADB	Android™ Debug Bridge

NOTE: Android is a trademark of Google LLC.

API	Application Programming Interface
-----	-----------------------------------

App	Application
ARP	Address Resolution Protocol
BYOD	Bring Your Own Device
CIS	Center for Internet Security
COPE	Corporate Owned, Personally Enabled
CSC	Critical Security Controls
CSF	Cybersecurity Framework
CVSS	Common Vulnerability Scoring System
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
EMM	Enterprise Mobility Management
GPS	Global Positioning System
GSMA	GSM Association
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ID	IDentification
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IMEI	International Mobile Equipment Identifier
IOS	Internet Operating System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
ISAC	Information Sharing and Analysis Center
IT	Information Technology
MAC	Media Access Control
MAM	Mobile Application Management
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MitM	Man-in-the-Middle
MTD	Mobile Threat Defense
NAND	NOT AND (memory)
NFC	Near Field Communication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NITS	Network Identify and Time Sone
Nmap	Network mapper
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
OTA	Over The Air
OWASP	Open Web Application Security Project
PC	Personal Computer
PDF	Portable Document Format
PIN	Personal Identification Number
SDK	Software Development Kit
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SMS	Short Message Service
SP	Special Publication
SSID	Service Set IDentifier
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network

4 Applying the Critical Security Controls for effective risk control and enhanced resilience of the mobile communications sector

4.1 Introduction, Methodology and Use

The security challenges facing the usage of mobile devices in the enterprise warrant additional attention. While many of the core security concerns of enterprise IT systems are shared by mobile devices and their management systems, unique challenges exist. For instance, mobile devices leave the physical and logical boundaries defined by an organization where normal workstations are maintained and physically secured. The diminutive form factor of a mobile device makes loss or theft a real concern, especially when these devices store proprietary and sensitive enterprise information that may also be governed by sector-specific regulations (e.g. healthcare data). Mobile devices are not the only type of device that regularly ventures outside the traditional enterprise network boundary (e.g. laptops). Users frequently connect phones and tablets to unsafe networks to perform work tasks, and subsequently bring the device back to the enterprise. Devices may also automatically connect to unsafe networks without the user's knowledge, which may then be brought back into the enterprise. Finally, users generally feel empowered to install mobile applications that a system administrator may have no knowledge of, yet will need to defend against.

Apple® iOS and Google Android™ OS are referenced as examples in this clause. However, the provisions apply to other mobile operating systems deployed for similar purposes.

NOTE: iOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used by Apple under license.

In order to defend against mobile threats, system administrators often rely heavily upon centralized management technologies such as Enterprise Mobility Management (EMM) and Mobile Device Management (MDM). These mobility management systems work to leverage the technologies built into mobile devices, and supplement this with their own proprietary approaches. System administrators face an important decision early on - how much control do they want users to have over these devices? A mobile device deployment model should be selected. Although requiring users to keep two phones on their person might be the easiest way to keep business information separate and secure, it is more expensive and reduces usability. Decreasing usability can lead to shadow IT.

The Bring Your Own Device (BYOD) model is often attractive to both administrators and users as it is a quick way to get users access to the information needed to perform their job. Yet, to properly secure this device usage model requires planning and the implementation of multiple layers of security defences. BYOD also makes it easy to infringe upon user privacy, either intentionally or by accident, leading some employees to request two distinct devices. Often times, one model may not be chosen for an entire organization. Different employees will have different needs and tolerances for security, privacy, and ease of use. This may be due to job function, privacy concerns, or simply personal preference. Supporting multiple models, alongside dealing with the legal and policy issues affecting BYOD, can be a challenge.

Besides how devices are provisioned to users, the apps that will be allowed to run on these devices are a major concern. Modern devices make it very easy to download and acquire new apps, with the mobile Operating System (OS) often actively encouraging users to do so. But downloading insecure or dangerous apps is a primary avenue for malware to infect a phone or tablet. The mobile application (app) stores try to prevent malware within their stores via app vetting programs, but they do not stop everything. Systems known as Mobile Threat Defense (MTD) can notify users and admins of dangerous apps as they are installed, and also detect attacks against the device itself. This technology can proactively help users make good security decisions about their devices and the apps they install. MTD can also help to detect phishing emails and text messages, alongside dangerous sites that a user may unintentionally be visiting. MTD often is developed and sold by a company separate from an EMM provider, but is sometimes viewed as a complement to that technology.

Mobile devices and apps face unique attacks and security concerns, and differ from traditional IT environments. The overriding themes for applying security for mobile devices are device management and configuration alongside the practical usage of cryptography, and careful controls and policy around the installation, usage, and data stored in mobile applications.

Methodology

A consistent approach is needed for analysing Controls in the context for mobile. For each of the Controls, the following information is provided:

- **Applicability:** The applicability field assesses the degree to which a Control functions within the mobile space.
- **Deployment Considerations:** Deployment considerations analyse if specific mechanisms are needed for a particular mobile deployment model, such as BYOD or fully-managed. Unmanaged deployment models are not addressed, as all mobile devices used for work tasks should be managed in some way, either via technical and/or procedural means, or via policy.
- **Additional Discussion:** This is a general area for any guidance that also needs to be noted. For instance, relevant tools, products, or threat information that could be of use can be placed here.

Relevant Enterprise Technology

This clause defines and describes the technology used to manage mobile devices.

- **Enterprise Mobility Management (EMM):** In its simplest form, an EMM is an over-arching term describing the plethora of systems available to manage, configure, track, and administer mobile devices in an enterprise. MDM and Mobile Application Management (MAM) are predominantly components of an EMM. Security Information and Event Management (SIEM) and MTD commonly integrate with EMMs. EMM systems can have full (e.g. admin, privileged) or partial control of a device. The Apple Device Enrolment Program (DEP) is an example of a fully-managed deployment scenario.
- **Mobile Device Management (MDM):** MDMs are the administration application primarily used to configure devices and set policies for mobile devices. MDMs typically have an on-device application that acts as the enterprise's foothold on an employee's device. This application is limited by the operating system in what it may and may not do. The mechanism of privileged actions is usually managed by OS APIs and granted OS permissions at installation time. MDMs may come with a suite of applications, including a secure container. They may also leverage custom, device vendor installed operating system level code in the Android™ environment to perform actions or enforce controls.
- **Secure Container:** A secure container is a device-side mobile app that provides a secure working environment to store enterprise data and prevent access from third-party apps. *These containers are a completely different technology from server-side containers such as Docker or Rocket.* Secure containers can be deployed on managed or unmanaged devices, and often have multiple apps contained within them from the same developer, such as a browser or email client. Containers may be implemented at the application level or integrated into the operating system itself.
- **Mobile Application Management (MAM):** MAM systems generally configure and manage mobile applications, and their focus rarely moves to the device itself. MAMs may integrate with an EMM, but may also be completely stand-alone solutions.
- **Mobile Threat Defense (MTD):** MTD is a form of mobile endpoint protection that generally identifies malware and attacks on the device. Additionally, they can be used to monitor URLs and messages within messaging apps for social engineering attacks or identify network-based attacks such as Secure Sockets Layer (SSL) / Transport Layer Security (TLS) stripping or Address Resolution Protocol (ARP) poisoning. The usefulness of MTD does vary from platform to platform with MTD providing maximum impact on Android.
- **Unified Endpoint Management (UEM):** UEM is an expanded form of EMM, providing the ability to manage traditional desktops and servers utilizing non-mobile platforms. This technology moves towards the *single pane of glass* for managing all devices in an enterprise. A single pane of glass is a management tool that brings together data from several different sources or interfaces and presents it in a single, unified view. An effective single pane of glass dashboard includes an intuitive Graphical User Interface (GUI) that is easy to navigate.

There are many ways in which the systems above can be integrated into an enterprise network. Many organizations will leverage cloud-based EMMs and direct employees to download the accompanying mobile app from a mobile app store to enroll their devices. The infrastructure for cloud-based EMMs is hosted and managed off-site, in the cloud, by the EMM vendor. Other organizations may view this as too risky of an endeavour and look to host their EMM within their own IT infrastructure. This is known as an on-premises, or on-prem, EMM architecture. Whether or not to host the EMM on-site or in the cloud may have impacts on the types of third-party integrations available and the security of enterprise mobile information. It is often one of the important early decisions when beginning a mobile device roll-out.

Mobility Deployment Model Descriptions

Organizations can choose to utilize one or multiple device deployment models. These models offer varying degrees of control and visibility to administrators and privacy to users. The technologies mentioned above can all be used within any deployment scenario listed below. The mobile deployment model to select for an organization varies based on risk appetite, budget, and job function. Other relevant factors include data sensitivity, ownership of the device, and the degree of separation necessary between enterprise and user data. It is possible that hybrid deployments will be necessary, giving some users a greater degree of latitude based on their job function. Some mobile product vendors both provide detailed guidance on managing their products. There are a large number of possible deployment models, but some of the more popular ones are:

- **Unmanaged:** Administrators can provide access to enterprise services (such as email, contacts, and calendar) to employee users without inspecting the device. Although a popular model for small companies and startups, this is the most dangerous scenario in terms of enterprise risk and it should be avoided. The present document does not address this deployment model.
- **Bring Your Own Device (BYOD):** Devices are owned by the end-user, or employee, but occasionally are used for work purposes. These devices should be permitted the least access to organization resources. BYOD devices could be joined directly to an MDM with end-user consent, but are more often managed through a mail and calendaring system such as Exchange ActiveSync. Access from BYOD devices to organizational resources are strictly controlled and limited. Common controls on the device such as storage encryption and requiring a passcode should be enforced. Employees own the device and can expect access to their organization's enterprise with little to no limitations on their overall device capabilities. Employees can also expect corporate data and/or the entire device to be remotely wiped in the case of it being lost, stolen, or an employee's departure from the organization. In some situations, depending on the sensitivity of an organization's data and the threat environment, BYOD can be safely achieved with remote wiping capability alongside a secure container to contain, protect, and delete the organization's data.
- **Corporate Owned, Personally Enabled (COPE):** COPE devices work in a similar fashion to BYOD, except the organization owns and furnishes the mobile device. Restrictions will be applied to the device but generally do not prevent most of what the user intends to do with the device. Although a COPE device is personally enabled, it ultimately belongs to the enterprise - *as does the information on the device*. The privacy and legal implications of an individual's data on the corporate device should be considered and addressed via information security policies. These devices are joined directly to an MDM with applications and access provisioned according to the user's role. Additionally, containerisation can be employed to separate the work and personal areas of the device. Despite containerisation, automatic updating of both the Operating Systems (OSs) and the applications should be enforced to the extent possible.
- **Fully-managed:** Devices within this deployment scenario are typically locked down and only permitted to perform business functions. Fully-managed devices are often owned by the organization as are all data residing on the device, necessitating that employees have a second device for personal use. These devices are centrally managed, which provides important security benefits but also presents usability barriers to employees. Devices owned and distributed for solely work purposes are both the most controlled and most trusted devices. These devices are provisioned directly to an EMM before a user has the device, and access provisioned according to the user's role. Automatic updating of both OS and applications is enforced to the extent possible, and the user is not able to install unapproved software.

Definitions and Scope

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 [i.17] defines a mobile device as:

"A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g. wirelessly transmit or receive information); possesses local, non-removable data storage; and is powered on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture (e.g. photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers".

The Cloud Security Alliance Mobile Working Group Guidance [i.18] defines mobile computing as:

"A very broad term which can be used to define any means of using a computer while outside of the corporate office. This could include working from home or on the road at an airport or hotel. The means to perform mobile computing could include kiosks used to remotely connect to the corporate office, home computers, laptops, tablets, or smartphones. Specialized or integrated devices could also be considered as mobile computing devices".

Both definitions are fairly broad and encompass a plethora of systems within their umbrella including smartphones and tablets. Ultimately, the present document defines mobile devices as distinct from the Internet of Things (IoT). Laptops, specifically 2-in-1 laptops, bridge the divide between traditional enterprise systems and tablets. Enterprises should choose whether these systems fall within the definition of mobile. It may be best to draw a distinction at whether a system can be managed by an EMM. For further discussion of the characteristics of a mobile device, see NIST Special Publication 800-124 [i.19].

The Critical Security Controls distinguish between "laptop" and "mobile" devices by labelling laptops and mobile devices as distinct types of portable devices.


Enterprise Mobility Management (EMM) Configurations

Benchmarks are available for some widely-used mobile device Operating Systems. See ETSI TR 103 305-4 [i.11], clause 9, Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms. These Benchmarks provide prescriptive guidance for establishing a secure configuration posture for both of the major mobile operating systems. These guides are tested against specific hardware and software versions of the mobile OS and are known to function as intended. While these guides are not specific to any EMM, they describe the security options offered by the platform and can act as a baseline set of recommendations for which security measures to put into place within an EMM. EMM vendors often reuse the same names for the security options, meaning it is fairly easy to identify these settings within an EMM.

4.2 Applicability Overview

Table 4.2-1: Applicability of the Critical Security Controls to the Mobile Sector

Control	Safeguard Title	Applicability
1	Inventory and Control of Enterprise Assets	
2	Inventory and Control of Software Assets	
3	Data Protection	
4	Secure Configuration of Enterprise Assets and Software	
5	Account Management	
6	Access Control Management	
7	Continuous Vulnerability Management	
8	Audit Log Management	
9	Email and Web Browser Protections	
10	Malware Defenses	
11	Data Recovery	
12	Network Infrastructure Management	
13	Network Monitoring and Defense	
14	Security Awareness and Skills Training	
15	Service Provider Management	
16	Application Software Security	
17	Incident Response Management	
18	Penetration Testing	

Control	Safeguard Title	Applicability
	More than 60 % of Safeguards Apply.	
	Between 60 % and 0 % of the Safeguards Apply.	
	0 %.	

4.3 Applying the Critical Security Controls and Safeguards

4.3.1 CONTROL 01 Inventory and Control of Enterprise Assets

Mobile Applicability

Tracking the systems with access to enterprise resources is critical, and the intentional mobility of these devices complicates this task. Similar to traditional workstations, insecure mobile devices can be used as a foothold to gain access to other enterprise systems. This creates unique challenges for mobile devices as they are not perpetually attached to the corporate network like a majority of IT assets, affording attack opportunities via unmonitored networks such as cellular connectivity or third-party Wi-Fi® networks of varying trustworthiness. Phones and tablets may be connected to the corporate network for part of a day, then not present for a week, or periodically checked-in when a Virtual Private Network (VPN) is enabled. This necessitates the use of multiple tracking methods to maintain the hardware asset inventory and ensure the device is still under control.

Mobile Deployment Considerations

All deployment models require hardware asset tracking. Note that active and passive asset discovery tools cannot help an organization identify the deployment model used for each device (i.e. if the device is BYOD, COPE, or fully-managed). This information should be stored in the detailed asset inventory:

- **BYOD:** BYOD devices are so sufficiently difficult to track that the *Controls* document [i.10] specifically calls out BYOD as presenting unique challenges. Organizations may wish to consider additional asset tracking mechanisms for BYOD devices due to high device turnover. Devices should be tracked alongside their deployment model (e.g. BYOD) and detailed device type. Tracking of hardware network addresses alone is insufficient to properly track BYOD mobile devices.
- **Fully-managed:** Fully-managed devices should also be tracked alongside their deployment model and detailed device type. As with BYOD, tracking of hardware network addresses alone is insufficient to properly track fully-managed mobile devices. Due to the greater degree of control organizations can exercise over fully-managed devices, it is possible to specify regular device check-ins and provision the device with whatever management software and configurations necessary to assist with hardware asset tracking.

Mobile Additional Discussion

Typical asset tracking tools may not work out-of-the-box with mobile devices. In order to properly track mobile devices, an additional plugin or purchase may be necessary. Mobile devices will respond to Network mapper (Nmap) scans but usually not in a manner that supports discovering the device's type. This is because the device rarely offers any service ports to connect to. Tracking Media Access Control (MAC) addresses can be difficult due to the MAC address randomization built into some mobile devices, which helps to protect a user's privacy when probing for or connecting to a network. Unfortunately, this feature can also actively prevent hardware asset management tools from properly tracking the device. At the very least, organizations can procedurally make a listing of mobile device hardware, device type, serial number, phone number, and other relevant information. All information about a device can be tied to an individual user account. Nmap is not designed to identify remote devices not connected to the enterprise network.

EMMs can support hardware asset tracking by installing agents on the mobile devices to apply configurations and security profiles, monitor devices for configuration changes, and monitor private access controls based on policy. The device would use any network it is connected to, to receive instructions and provide status information. Privileged EMM agents can obtain and report detailed hardware configuration information back to the enterprise that can be obtained via the primary EMM console. Device location via Global Positioning System (GPS) can also be tracked within an EMM, but this can infringe on a user's privacy. The EMM console may be able to integrate with an organization's primary asset management platform.

Table 4.3.1-1

Control 1: Inventory and Control of Enterprise Assets				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	•	•	•	Y	Hardware inventories are important for any device accessing the enterprise network, and mobile devices should be included in this inventory. Alongside the information listed in the text of the Safeguard, telephone number, International Mobile Equipment Identifier (IMEI), device hardware model, and deployment type (e.g. BYOD, fully-managed) should also be tracked. Bi-annual status for a mobile device seems very long for these easy to lose or steal devices. Encourage reporting by the user of suspected loss within four hours.
1.2	Devices	Respond	Address Unauthorized Assets	•	•	•	Y	Unknown mobile devices connected to enterprise assets should be quickly removed via an approved process. Devices as well as authorized services should be addressed, such as logging into an email account on an unauthorized device. In some organizations, connecting a mobile device via a cable to an organization asset, as is done when charging a phone from the USB port of a computer, may represent an unacceptable risk.
1.3	Devices	Detect	Utilize an Active Discovery Tool		•	•	Y	Although active discovery tools may not always work perfectly for mobile devices, they can generally be upgraded and further configured in order to function as needed. A better path forward for active discovery would be to place an EMM or other application onto the device to obtain hardware inventory and other useful enterprise information.
1.4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		•	•	Y	Although this is possible, by itself it is not considered an industry-accepted method of tracking mobile device inventory and should not be the primary method in which mobile devices are tracked.

Control 1: Inventory and Control of Enterprise Assets				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
1.5	Devices	Detect	Use a Passive Asset Discovery Tool			•	Y	<p>A passive asset discovery tool would likely be suboptimal, but still provide useful information for mobile devices.</p> <p>The most likely opportunity to passively observe mobile devices on an organization-controlled network is through HTTP/HTTPS traffic. The user-agent field of a web request can provide an effective differentiator for mobile devices. The opportunity to see this web traffic, however, is diminished greatly when strict transport security control is enforced by the mobile operating system, effectively suppressing plain text HTTP traffic.</p>

4.3.2 CONTROL 02 Inventory and Control of Software Assets

Mobile Applicability

Software assets to be tracked include a mobile device's firmware, OS, and apps. A mobile OS is tailor-made for specific smartphones and tablet hardware platforms, and leverages firmware from a variety of sources in order to enable peripherals and sensors. Expanding to the larger mobile ecosystem, there are millions of mobile applications available to download and install across the mobile platforms. Although widely-used mobile operating system app stores screen mobile apps for security issues, their application vetting mechanisms are not foolproof.

Furthermore, users could download apps from both legitimate third-party app stores and stores delivering cracked or pirated software. Regardless of their provenance, mobile apps from any source can threaten the security of enterprise data and credentials. IT professionals with responsibility for a company's mobile footprint should understand the apps, and specifically should know which version is important to protect the organization. Outdated firmware and software often contain exploitable vulnerabilities that an attacker could leverage to access enterprise data.

Mobile Deployment Considerations

Obtaining the name and version of an app for an organization's software inventory can vary based on the mobile deployment model in place:

- **BYOD:** BYOD deployments using a secure container application may be unable to obtain detailed app version information for installed apps outside of the container. Within iOS, unprivileged applications cannot read the listing of apps on a device. Therefore, a secure container alone may be insufficient to create a software asset inventory of the apps for BYOD deployments. An EMM / MDM with an agent installed on the device would be necessary to obtain both a listing of apps, and app version information. An EMM agent will also be able to provide detailed operating system information. On Android, an MTD application will be able to obtain the necessary information. Removing unauthorized apps is technically and procedurally difficult in BYOD deployments unless a secure container is in use, but is limited to removing the applications and its data installed within the secure container. Finally, consider defining a minimum acceptable mobile OS version, and updating this practice every six months.
- **Fully-managed:** Creating a software asset inventory for fully-managed devices should not be a difficult task, provided that the organization is leveraging an on-device EMM agent. Removing unauthorized apps is feasible in fully-managed scenarios.

Mobile Additional Discussion

Mobile devices have firmware and software running across the device stack. It can be difficult to obtain baseband and other firmware information and this will likely be untracked by an enterprise. The mobile device manufacturers actively thwart extraction of on-device OS, hardware, firmware, and baseband components by removing administrative access from the device owner and physical restriction of direct storage extraction. Tracking OS and application versions of Bluetooth® and Wireless Fidelity (Wi-Fi) devices can be quite difficult and may not be possible using traditional scanning methods. Applications like Airmon for Wi-Fi devices and hcitool or ubertooth-scan for Bluetooth devices will at best provide broadcast advertisements and MAC addresses. Note that Bluetooth MAC addresses do not conform to typical conventions and are often represented as the device Wi-Fi MAC address incremented by 1 bit.

Allowlisting is a built-in capability on iOS and Android, but this is only for mobile apps. It is not extended to external software libraries and scripts. On Apple iOS, applications are digitally signed with that signature verified on install and at every execution of the program. Unsigned libraries on iOS will not execute without a valid code signing certificate. With Google Android, apps are digitally signed but the signature may not necessarily be checked on all platforms and versions of Android. Further, the Android signature mechanism is focused on protecting the installed application from updating by a malicious version of that application. Additional information is available via OS developer pages and security guides.

Table 4.3.2-1

Control 2: Inventory and Control of Software Assets				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
2.1	Applications	Identify	Establish and Maintain a Software Inventory	•	•	•	Y	At a minimum, mobile device operating system and application information such as application package name and version should be tracked. This is most easily done if an enterprise has a presence on the mobile device via an EMM or similar mechanism.
2.2	Applications	Identify	Ensure Authorized Software is Currently Supported	•	•	•	Y	Some EMMs have the capability to alert administrators if an app is out-of-date or no longer supported. Another option would be setting a compliance policy to alert the administrator if an app is being used that is not part of an administrator specified allowlist. MTD agents may also have this capability. A mobile application vetting process can also assist with ensuring apps are supported. The mobile OS itself is almost never the latest on each device. The latest OS version available for that device should be installed. Further, the organization should select phone models for deployments where it controls the device selections that tend to receive Android updates rapidly. UEM solutions have the capability to have their own "App Store" for the work container with only approved apps. This allows the personal space to install whatever they want.
2.3	Applications	Respond	Address Unauthorized Software	•	•	•	Y	Software that is not approved by the enterprise should be removed. Automated removal of apps is not always possible. Some UEM solutions can notify the user that they are non-compliant, block unapproved apps from installing, and/or only allow installation from the UEM's App Store.
2.4	Applications	Detect	Utilize Automated Software Inventory Tools		•	•	Y	EMMs act as a software inventory tool by providing visibility into enterprise-owned devices, and helping to track and coordinate mobile devices.

Control 2: Inventory and Control of Software Assets				Implementation Groups			Applicability	
2.5	Applications	Protect	Allowlist Authorized Software		•	•	Y	Major mobile operating systems generally perform some degree of application-level allowlisting by default. This can be subverted by malicious MDM profiles or insecure system settings. Malicious MDM profiles can trick a user into providing access to an unauthorized entity or allow the installation of dangerous applications. Insecure OS settings, such as the "Allow Unknown Sources" on Android, can allow for the installation of dangerous and insecure apps.
2.6	Applications	Protect	Allowlist Authorized Libraries		•	•	N	Allowlisting individual libraries is not typically available on widely-used mobile operating systems.
2.7	Applications	Protect	Allowlist Authorized Scripts			•	N	Allow listing individual scripts is not typically available on widely-used mobile operating systems.

4.3.3 CONTROL 03 Data Protection

Mobile Applicability

Control 3 is a combination of technical and procedural methods for ensuring data is not accessed by unauthorized entities. It begins with establishing a program to manage how data is classified, stored, and protected throughout the enterprise. It also includes understanding data flow and how data is retained. Mobile data can be managed, detected, and retained in similar ways to traditional enterprise data, although it may take additional resources and specialized knowledge to do so. Understanding how a mobile life cycle applies to your organization can help, which can include device acquisition, configuration, provisioning, usage, updating, and sunset.

Many types of traditional mobile data can be found on mobile devices, such as business email, contacts, and calendar. Additionally, mobile devices generate mobile-specific information such as call logs, text messages, and mobile app data, all of which needs to be managed and protected according to sensitivity. The fact that mobile devices have such a diverse supply chain and utilize numerous cloud services by default makes *Data Protection* an even more difficult task. Yet steps can be taken to protect enterprise data on mobile platforms, as a variety of mitigations can be put into place for these systems.

Mobile Deployment Considerations

Allowing contractors and employees to access enterprise systems with their own devices leaves the enterprise without visibility into the device and how enterprise data is being handled. It is difficult to gain assurance of the security of data on mobile platforms without some sort of enterprise presence on a device:

- **BYOD:** Within the traditional BYOD, use case employees want to use their own device, requiring stronger levels of control and device posture assessments to be performed and maintained by the enterprise. Organizations with BYOD programs will need to consider end-user privacy implications within policies and security monitoring and operations procedures. Additionally, agents on the device should not prevent users from accessing their own data, or affect other device operations. When removing a device from a BYOD program, assurance of secure data erasure of enterprise data is difficult to achieve if a secure container or dedicated enterprise mobile app is not in use; therefore, a secure container deployment is recommended.
- **Fully-managed:** Data protection policies are significantly easier to implement in fully-managed scenarios. All of the Safeguards in *Data Protection* below can be implemented, although some mobile-specific technologies will need to be leveraged.

Mobile Additional Discussion

Mobile devices have built-in APIs to leverage traditional VPN services. Mobile-specific VPNs are also available for accessing the enterprise network / gaining an internal IP address. Many modern UEM solutions also have built-in VPN capability for the work container to connect back to the corporate network. This ensures that corporate data passes through the necessary security controls such as next-generation firewalls and other systems monitoring the network. A large majority of mobile apps will attempt to store data in the cloud by default. This makes data protection difficult, as enterprises may not have visibility into how individual apps are configured, and depending on their access rights, may not even know which apps are installed on a device. Therefore, data storage locations should be analysed for multiple devices' deployment scenarios. Understanding where and how enterprise mobile data is being stored is very difficult. Administrators interested in that question should reference *Control 15: Service Provider Management, below*.

Traditional guidance on encrypting data on the devices, and using a VPN with standardized cryptography for protecting sensitive data in transit, still applies to mobile. There are VPNs that allow mobile devices to connect to corporate networks to access applications or data shares, as well as application-specific VPNs that encrypt the data in transit for that application. Some of these technologies include a hardware component, such as a microSD chip, for encryption key management. Traditional enterprise Data Loss Prevention (DLP) can be helpful for email, cloud, and network stored data. Yet cloud applications and data may be more difficult to get visibility from mobile device and user access. There are tools that leverage cloud service APIs to gain this visibility, or filtering software in clouds that proxy mobile users to these external services, which can provide a source for data access controls.

Table 4.3.3-1

Control 3: Data Protection				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
3.1	Data	Identify	Establish and Maintain a Data Management Process	•	•	•	Y	Elements of the data management process can apply to mobile. It is possible that these can be addressed as a subcomponent of a Mobile Security Policy, or possibly addressed as part of Data Management.
3.2	Data	Identify	Establish and Maintain a Data Inventory	•	•	•	Y	Sensitive information on mobile devices should be inventoried, such as emails, work-related text messages, calendar information, call logs, and contacts.
3.3	Data	Protect	Configure Data Access Control Lists	•	•	•	Y	IT administrators can control access and lifetime of accounts via administrative consoles. Users will generally have access to all data on a mobile device.
3.4	Data	Protect	Enforce Data Retention	•	•	•	Y	IT administrators can control access and lifetime of accounts via administrative consoles. Because many apps on mobile devices leverage these same accounts, access can be controlled. Data itself can be deleted via app-specific administrative functions or by keeping all work data within an enterprise-owned app for BYOD. Minimizing data downloaded to the mobile device for processing to only that which is necessary for a specific task, and aggressively expiring local copies of unneeded data, can be implemented by a corporate application. Fully-managed devices can simply be remotely wiped.
3.5	Data	Protect	Securely Dispose of Data	•	•	•	Y	Mobile devices often provide a cryptographic wipe, and a more traditional device wipe functionality. Both of these can be leveraged to dispose of mobile data. What is actually removed is device-dependent and OS-dependent when "wiping" the device. The decryption keys only may be wiped, leaving encrypted data on the storage media. Encryption provides protection against unauthorized access, but there remains a risk that it can be recovered.

Control 3: Data Protection				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
3.6	Devices	Protect	Encrypt Data on End-User Devices	•	•	•	Y	The NAND storage of mobile devices is typically encrypted by default, although some configuration (sometimes setting an authentication PIN is enough) is necessary by the user.
3.7	Data	Identify	Establish and Maintain a Data Classification Scheme		•	•	Y	Data classification decisions should be explicitly made for mobile data, specifically call logs, text messages, email, contacts, and calendar.
3.8	Data	Identify	Document Data Flows		•	•	Y	The enterprise should understand how sensitive data is transferred to and from mobile apps and devices. Understanding how the data is stored on the device should be part of the data flow, and app-level protection using hardware backed key escrow should be implemented for sensitive data.
3.9	Data	Protect	Encrypt Data on Removable Media		•	•	Y	This generally does not affect mobile devices as USB storage devices are still not widely utilized, but this is beginning to change with high-end mobile devices beginning to accept removable USB-C devices. Removable SD cards within phones were popular in the past but this is no longer the case. If an EMM offers these management capabilities, they should be leveraged.
3.10	Data	Protect	Encrypt Sensitive Data in Transit		•	•	Y	The use of mobile VPNs, and even per-app VPNs, can help to protect sensitive information in transit. Mobile apps also need to utilize encryption for communicating with both the enterprise and any management infrastructure. This Safeguard can also apply to the security of messaging platforms and voice traffic.
3.11	Data	Protect	Encrypt Sensitive Data At Rest		•	•	Y	The NAND flash storage of mobile devices is typically encrypted by default by the mobile OS. There are sometimes actions that the user needs to take.
3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity		•	•	Y	Using an enterprise-controlled mobile application, or suite of apps, is recommended for BYOD deployments. Fully-managed devices meet this Safeguard by being used solely for work functions.

Control 3: Data Protection				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
3.13	Data	Protect	Deploy a Data Loss Prevention Solution			•	Y	Traditional enterprise Data Loss Prevention (DLP) can be helpful for email and network-stored data, but cloud applications and data may be more difficult to get visibility from mobile device and user access. There are tools that leverage cloud service APIs to gain this visibility, or filtering clouds that proxy mobile users to these external services, which can provide a source for data access controls.
3.14	Data	Detect	Log Sensitive Data Access			•	Y	EMMs can log device access and adherence to compliance policies. Developers can also log changes to sensitive data access within their applications.

4.3.4 CONTROL 04 Secure Configuration of Enterprise Assets and Software

Mobile Applicability

Similar to traditional desktop and server platforms, mobile devices need to be configured. The correct configurations and monitoring of these configurations are critical to maintaining trust and security in a mobile deployment. These configurations can apply to devices, EMMs, applications, and the platforms used to manage and develop mobile technologies. Configurations could also be stored within standardized profiles containing configurations and compliance actions. Mobile devices are most often configured via EMM profiles, but in instances where enterprises do not have a presence on the device, users should be asked to configure specific settings themselves.

Mobile Deployment Considerations

The National Information Assurance Partnership (NIAP) approves EMM and MDM products, and may have detailed configuration guidance for the EMMs if a product's developer decides to achieve certification. Note that these configurations only apply to "on-prem" EMM deployments.

When developing mobile policies and creating configuration baselines, each organization should consider the usability impacts of the configuration settings before pushing them to devices.

BYOD: BYOD deployments should balance security with the usability impacts that employees are willing to take on their personal devices. Preventing the usage of third-party app stores may be tenable, but restricting content, such as the viewing of "R" rated movies on a personal device, may not be tolerated by the user. Benchmarks [i.11] can be tailored for BYOD scenarios.

Fully-managed: These scenarios can be significantly more "locked down" than unmanaged or partially managed scenarios. Benchmarks for widely-used operating systems can be directly used for fully-managed scenarios.

Mobile Additional Discussion

EMMs can configure application and operating system settings on mobile devices. Additionally, in fully-managed situations they can restrict user access to mobile device functionality such as cameras, allowlist Wi-Fi networks, apply password policy enforcement, apply VPN requirements, and inventory which apps are installed. Organizations obtaining privileged access to user devices should be aware of the privacy concerns associated with doing so. A company may not want the liability of knowing or having access to an employee's personal email, apps that track health information or financial data, personal contacts and calendars, apps used in their personal lifestyle, or their location.

Table 4.3.4-1

Control 4: Secure Configuration of Enterprise Assets and Software				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	•	•	•	Y	Organizations may choose to use Benchmarks [i.11] for configuring widely-used operating systems. The U.S. government NIAP program can assist with configurations for EMM and MDM applications.
4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	•	•	•	N	Mobile devices do not often need dedicated network devices, but dedicated VPN concatenators are possible to see. Mobile network infrastructure is out of scope for the present document.
4.3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets	•	•	•	Y	Automatically restricting access to the device is configurable in each deployment mode on all platforms, and is also modifiable by a user without specialized software.
4.4	Devices	Protect	Implement and Manage a Firewall on Servers	•	•	•	N	There are no mobile considerations for this Safeguard.
4.5	Devices	Protect	Implement and Manage a Firewall on End-User Devices	•	•	•	Y	Mobile devices do not typically contain an on-device firewall. Some vendors are beginning to offer this technology which should be considered.
4.6	Network	Protect	Securely Manage Enterprise Assets and Software	•	•	•	Y	Organizations developing mobile applications and infrastructure should use modern, secure management protocols. Organizations should ensure that applications selected for management of the deployed devices utilize secure transport protocols.
4.7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software	•	•	•	N	This is typically not a concern with mobile devices, unless the device is rooted or jailbroken.
4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		•	•	Y	Users should be educated on the implications of obtaining and installing mobile apps from insecure locations, or on iOS signed with developer or enterprise signatures.
4.9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets		•	•	Y	Configure trusted DNS servers on network infrastructure. Example implementations include configuring network devices to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.
4.10	Devices	Respond	Enforce Automatic Device Lockout on Portable End-User Devices		•	•	Y	Automatically locking after a predetermined number of failed device access attempts is a device API available on all platforms, and is also modifiable by a user without specialized software.

Control 4: Secure Configuration of Enterprise Assets and Software				Implementation Groups			Applicability	
4.11	Devices	Protect	Enforce Remote Wipe Capability on Portable End-User Devices		•	•	Y	Remotely wiping mobile devices is a critical capability for mobile device usage in the enterprise. This could be device wipe or a more targeted enterprise data-only wipe.
4.12	Devices	Protect	Separate Enterprise Workspaces on Mobile End-User Devices			•	Y	Separating work and personal information on a shared device is a best practice. It provides practical data separating and can also help alleviate privacy concerns. With that said, Android is multi-user by default. This could be leveraged in BYOD scenarios without Android for Work.

4.3.5 CONTROL 05 Account Management

Mobile Applicability

Account management is applicable to mobile devices and their management platforms. This Control is primarily enforced at the back-end management systems, and not within the device, although users do play a role within this Safeguard by creating and using unique passwords wherever possible. Enterprises may choose to use identity service providers to authenticate users, raising the bar for both security and usability in the process. Yet administrative privilege should also be directly managed.

Administrative privilege functions differently within mobile operating systems. Both Android and iOS allow for EMMs and MDMs to take administrative control of a device. The user can generally override administrative access by revoking their control, while in other situations this is not possible (such as with the Apple Device Enrollment Program). Administrators do not need to input an administrator password into a mobile device. Instead, the EMM dashboard is used to extend invitations to individual users and their devices. This dashboard is typically a publicly accessible web application and should be the focus of protecting the administrative level privileges over mobile devices. Messaging from the EMM app to the device should be cryptographically signed to ensure legitimate commands are delivered to enrolled/controlled devices.

Mobile Deployment Considerations

It is more difficult, or sometimes not possible, for enterprises to monitor accounts on unmanaged devices. On-device EMM agents can give enterprises access to the list of applications on the device, which can make it easier to monitor which third-party applications are being utilized. However, application-specific accounts are typically inaccessible. Many aspects of this Control apply to all mobile device deployment models:

- **BYOD:** Secure account management is very difficult to achieve without on-device presence for BYOD deployments. Leveraging an identity service provider for BYOD can be an excellent way of significantly securing access to enterprise resources.
- **Fully-managed:** All of the Safeguards provided below can be implemented, but account service providers need to take additional steps themselves in order to achieve this Control.

Mobile Additional Discussion

A documented process should exist for onboarding new users regardless of deployment scenario, likely spearheaded by IT. EMM administrators should routinely review the list of accounts with mobile access and disable any accounts not in use based on an expiration time from last use. Using an identity service provider or federating existing identities to mobile devices and the services they need to access can help alleviate many of the pains associated with mobile authentication. Fewer accounts will need to be managed and inventoried.

Table 4.3.5-1

Control 5: Secure Configuration of Enterprise Assets and Software				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
5.1	Users	Identify	Establish and Maintain an Inventory of Accounts	•	•	•	Y	Although an important Safeguard, there are no mobile-specific considerations. Each mobile device will be required to have an account for their device manufacturer's ecosystem. EMMs will by default have administrative accounts.
5.2	Users	Protect	Use Unique Passwords	•	•	•	Y	Although an important Safeguard, there are no mobile-specific considerations. As with all administrative functions, administrative accounts for management applications should use unique authentication credentials on mobile devices. Employees should use unique passwords.
5.3	Users	Respond	Disable Dormant Accounts	•	•	•	Y	In a manner similar to traditional systems, dormant accounts should be disabled after a pre-defined period of inactivity.
5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	•	•	•	Y	Administrative accounts for management applications should have dedicated passwords. Add a second factor of authentication whenever possible. It is noteworthy that the mobile device itself is frequently now the second factor of authentication (via SMS, a "soft token" app, or a "push verification" app) for the user's enterprise account. Scheduled auditing of administrative accounts should be regularly performed to assess if admin accounts / privileges are still required.
5.5	Users	Identify	Establish and Maintain an Inventory of Service Accounts		•	•	Y	Use of an administrative EMM account would obviate the need for local administrative accounts on mobile.
5.6	Users	Protect	Centralize Account Management		•	•	Y	EMMs can integrate with identity service providers, or may provide their own identity service.

4.3.6 CONTROL 06 Access Management Control

Mobile Applicability

Access Control Management is very applicable to mobile devices. While establishing a mobility program and securely provisioning devices to users is important, this Control is primarily concerned with managing existing mobile users' access to enterprise resources and ultimately revoking access. Thorough implementations of Control 5 and Control 6 involve written policies addressing these areas before devices are provided to users, although that is not always practical with existing user bases.

Mobile Deployment Considerations

The following describes general considerations for assigning privileges to different mobile deployment models:

- **BYOD:** In general, organizations should err on the side of assigning BYOD users fewer privileges than other deployment models. Access should be provided through pre-determined methods approved by security professionals. This is largely due to enterprises lacking the ability to lock down the device and monitor its health. Another consideration is that these devices are often remotely provisioned into the enterprise, without any physical presence or frame of reference for IT. If a secure container is deployed, some consider it prudent to automatically delete the data within the container after a defined period of time if the container cannot reach the management server.
- **Fully-managed:** In-person provisioning, regular device status check-ins, and complete configurations are all reasons to feel comfortable providing additional resources to fully-managed devices. Some consider it prudent to automatically delete the data within the device after a defined period of time if the container cannot reach the management server. The same can be said for aggressively wiping data and accounts that have not successfully connected to the management service in a defined period of time.

Mobile Additional Discussion

Administrators should regularly review user accounts on all systems utilized by the enterprise. Privileges should be adjusted accordingly on a regular basis with over-privileged users losing access and unneeded accounts deactivated when necessary. Users should be regularly prompted to authenticate to services, with MFA being a regular requirement for most services. Authenticating to a service on a mobile device often makes MFA much easier than traditional desktop / laptop environments unless hardware tokens are issued.

Cloud-based applications supported by the enterprise should be monitored and have their credentials disabled during employee separation. Enterprise apps should be analysed and reviewed for proper authentication techniques. Special attention should be focused on areas where integration occurs between third-party services and when identities are federated. Logging should be enabled within back-end management services to monitor activity, with the logs regularly reviewed.

Table 4.3.6-1

Control 6: Access Control Management				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
6.1	Users	Protect	Establish an Access Granting Process	•	•	•	Y	Written policies should exist for onboarding new mobile devices and users onto the network. This process can be semi-automated for UEM registration. They should be added to appropriate security groups. Registration to the manage application often happens with a QR code sent to their email account.
6.2	Users	Protect	Establish an Access Revoking Process	•	•	•	Y	In addition to typical workstations and servers, administrators should define this process specifically for mobile devices and their management platforms. Devices should be configured to self-revoke local data if connection to the management server cannot be established for a period of time.
6.3	Users	Protect	Require MFA for Externally-Exposed Applications	•	•	•	Y	Although not all applications support MFA, where possible it should be performed. Mobile devices will often act as an authenticator for MFA. Note that MFA for the lock screen is out of scope for this Control. Where it is provided as part of the operating system, it should be configured and used. This is currently implemented as a push notification to other places where the iCloud or Gmail account holder is logged in.
6.4	Users	Protect	Require MFA for Remote Network Access	•	•	•	Y	VPN applications and their back-end components can integrate with external authentication services and identity providers. To the degree possible, enterprises should refrain from using a phone number as an identifier, as this can be used to enable personal attacks. Note that SMS-based one-time passwords are considered weaker than many other MFA systems, and should be avoided if possible.
6.5	Users	Protect	Require MFA for Administrative Access	•	•	•	N	2FA is not always supported when provisioning a device into an EMM. 2FA should be implemented if a tool offers it.
6.6	Users	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems		•	•	N	Although an important Safeguard, mobile-specific authentication systems are not commonplace.
6.7	Users	Protect	Centralize Access Control		•	•	N	This is difficult to accomplish when mobile OS vendor accounts are necessary to enable even basic mobile device functionality.

Control 6: Access Control Management				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
6.8	Data	Protect	Define and Maintain Role-Based Access Control			•	Y	EMMs provide the ability to provide user roles with profiles appropriate for the specific role of the user. Utilize this capability.

4.3.7 CONTROL 07 Continuous Vulnerability Management

Mobile Applicability

Mobile vulnerabilities are often linked to versions of the mobile OS or apps installed on the device. Misconfigurations of the mobile OS or installed apps also fall within the scope of this Control. Since mobile devices are not always attached to the corporate network, it is difficult to identify and manage vulnerabilities in a manner similar to how one would on desktop workstations, servers, or network appliances. Traditional vulnerability management products may not act in a predictable manner unless the products are specifically geared toward mobile. These traditional tools often require additional plugins that should be separately purchased to enable mobile device vulnerability scanning. Separate products may exist for scanning the EMM and MDM systems and mobile devices themselves. Some vulnerability scanners may only function by directly integrating with an EMM for device access or may require an agent-based solution to be installed. Understanding the limitations and bounds of use for mobile device scanning is necessary before purchasing a product.

Vulnerability management on mobile devices often takes the form of application assessment. This task is infrequently performed by an organization, instead relying on the mobile device OS vendor to scan applications prior to their inclusion in the corresponding app store. Vulnerabilities are thus undiscovered, discovered by security researchers, or discovered in root cause analysis of a security incident or breach.

Mobile Deployment Considerations

Traditional vulnerability scans are not the primary method that IT administrators use to obtain vulnerability information about their mobile devices. Vulnerability scanning tools often require that devices are on the same subnet in order to be scanned, and this is not often the case for mobile with users primarily using their devices outside the network boundary. An exception would be a mobile VPN providing a mobile device with an IP address on the enterprise network:

- **BYOD:** Vulnerability management on BYOD devices is difficult. Users will often need to be reminded to update either device. Organizations may wish to utilize additional agent-based MTD tools with devices that are not provisioned into an EMM.
- **Fully-managed:** Organizations with privileged access on the device can install agents that can access the name, and possibly developer, of each app installed on the device. In fully-managed scenarios, these apps can be pushed and configured for the device.

Mobile Additional Discussion

Vulnerabilities and misconfigurations within mobile devices can apply to many layers of the device stack:

- **Hardware** - Such as within a processor improperly utilizing speculative execution.
- **Firmware** - As would be the case within the firmware used to power a camera.
- **Operating system** - Such as a memory management error within an OS kernel.
- **OS library or subsystem** - For instance, if a file header was improperly read and sanitised, executing instructions contained within the header.
- **Application** - Over-privileged mobile apps may steal sensitive information, such as a user's location or contacts, and send it back to the application's central storage location. This may be a legitimate app that exceeds the boundaries of appropriate use for the organization.
- **Communications protocol** - Any communications protocol utilized by the device, such as cellular, Bluetooth, Wi-Fi, and Near Field Communication (NFC).

These are a few examples, with the mobile threat surface expanding out to the entire ecosystem used to empower mobile devices nowadays. Many intrusions use valid credentials obtained through external means, such as social engineering. One important consideration in mobile is protecting credentials stored on the device, because a user's email account could also serve as their system or Domain Admin account. Self-service password resets often use an email message to authorize a password reset, resulting in escalation of the attacker's control of a compromised user's information system assets.

MDM tools can scale to hundreds of thousands of devices, and provide the necessary monitoring to be alerted when devices are out of compliance; for instance, if someone installs an unauthorized application, turns off encryption, or jailbreaks or roots their device. (Jailbroken and rooted tools often deploy masking of the compromise of the device to intentionally thwarting the EMM and MDM detections.) By default, these monitoring tools do not continuously scan, instead scanning at a predetermined interval. Successful attacks on a device occurring during this period of time between scans would not be noticed by the enterprise until the next scan is run. The scan period is configurable, but frequent scans can come at a cost of significant power utilization. Mobile vulnerability assessments should incorporate threat modelling and an understanding of the devices, data, users, and their behaviours. MDMs can play a key role in gathering the information for the "what" and "who" for mobile management, listed in Controls 1 and 2, that provide the foundation for this Control. Vulnerabilities can sometimes be identified and managed within EMMs and MDMs via traditional vulnerability managed scanners and other tools.

Mobile security tools using an agent-based approach give a view to threats on and to the mobile device, such as malicious applications and profiles, malicious Wi-Fi networks, or Man-in-the Middle (MitM) web proxy attacks. There are also tools and approaches that funnel mobile traffic through filtering cloud infrastructures that perform web gateway filtering and security functions. Some EMM vendors may use browsers that they have additional control over. These browsers may be home-brewed, or utilize important libraries and kits from other on-device browsers.

Mobile operating systems, email clients, browsers, and all apps should be kept up-to-date in order to remain effective because the OS manufacturer, Original Equipment Manufacturer (OEM), and baseband provider (e.g. Qualcomm, Intel) all have to work together to develop, approve, and authorize mobile OS updates. It can take significant time to receive these updates, if they will be made available at all. When an update is available, admins cannot generally force an update, but can let a user know that an update is available and that they should install it. This can be done via an on-device notification through the management app / secure container, or through more traditional means (e.g. email, word-of-mouth). Additionally, it should be noted that the Android ecosystem has an operating system update issue, where not all deployed Android devices will get updates in a timely fashion (if at all). The core of this issue is that updates to the operating system go to the vendors and mobile operators for customization prior to deployment to the actual phones. The situation is being addressed in newer Android OS versions (Android 10 and later) getting updates via the application deployment model and abstraction of vendor code from operating system components.

Table 4.3.7-1

Control 7: Continuous Vulnerability Management				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
7.1	Applications	Protect	Establish and Maintain a Vulnerability Management Process	•	•	•	Y	Existing vulnerability management processes should include mobile devices, including their operating systems and installed applications.
7.2	Applications	Respond	Establish and Maintain a Remediation Process	•	•	•	Y	Vulnerability processes for mobile devices often involve updating software from the carrier, OS developer, or mobile app developer.
7.3	Applications	Protect	Perform Automated Operating System Patch Management	•	•	•	N	Unless a particular fully-managed scenario is used, external tools are often unable to force updates to the mobile OS. This depends on the OEM and possibly cellular provider to provide Over The Air (OTA) updates. Administrators are often able to remind users to update their phone via a notification.
7.4	Applications	Protect	Perform Automated Application Patch Management	•	•	•	N	Unless a particular fully- managed scenario is used, external tools are often unable to force updates to the application. Administrators are often able to remind users to update their apps via a notification. A mobile application has the ability to check to see if it has expired. Favor applications disable themselves if they are not the latest version. This is especially important in the case of serious flaws. A phased approach may be favoured where an older version will continue to run unless there is a serious issue identified.
7.5	Applications	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets		•	•	N	Mobile vulnerability detection tools often use an on-device agent, which is neither an authenticated nor an unauthenticated scan.
7.6	Applications	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		•	•	N	This has no applicability to mobile devices. Some tools may allow for mobile applications to be potentially automatically scanned.
7.7	Applications	Respond	Remediate Detected Vulnerabilities		•	•	Y	Forcing OS and mobile app updates at a specific time is not always possible, although settings for automatically updating software can be enabled. This should lead to a timely update process. Note that this setting may cause service interruptions if important services (e.g. email) become incompatible during the update process.

4.3.8 CONTROL 08 Audit Log Management

Mobile Applicability

Mobile devices do not generate logs in the same manner as traditional desktop devices. If and when logs are generated, they are not necessarily made available to an external application or service. Widely-used operating system logs do exist, and can most often be obtained after a device syncs with a desktop and may need to be manually pulled from the device. Mobile apps may generate logs as well, but this will be a design decision made by the developer and is not commonly available to the enterprise.

Mobile Deployment Considerations

The following describes general considerations for obtaining audit logs in different mobile deployment models:

- **BYOD:** Audit logs are generally unavailable on BYOD platforms without an enterprise presence on the device. A secure container or similar application may provide the ability to pull logs from the device or specific applications, often developed by the same company.
- **Fully-managed:** These scenarios will provide additional access to mobile OS and application logs resident on-device. These logs are separate from EMM tools, which generate their own bodies of logs and can integrate with a SIEM. SIEMs can ingest and correlate events between all available data sources, such as apps, devices, UEM, EMM, MDM, MTD, and other mobile information sources. If a management solution has a VPN enabled, all traffic can be funnelled to the corporate network. This will allow for full network visibility of everything in the work container and enable use of all corporate security controls.

Mobile Additional Discussion

Monitoring is irrelevant if there is not a process to identify events and respond to them. And this response should be matched with the potential impact of the event. This is the human aspect: determining which events or alerts can potentially damage the organization, and executing a response in a timely fashion based on that. Varying sources of mobile data can be monitored. MDMs use the more traditional network operations type of approach and try to answer the following questions: *Is the device live? What is the make, model, and version? Is it up-to-date? Which applications are installed? Has the device been rooted or jailbroken? How much traffic is it sending and receiving?* Many of these items can be set up via compliance policies.

Traditional security tools have more granular logging, such as installation of known bad or suspicious desktop applications, application-level changes to data, network routing changes, SSL certificates used, Virtual Private Network (VPN) launching, and, in the case of cloud filtering, traditional perimeter gateway logs for web traffic, or other application traffic. There is also the practice of monitoring account connections to the network domain or a specific application.

Logs can be used to create cybersecurity and technology metrics. Metrics should be actionable in lieu of providing solely the number of occurrences for an event. More effective things to track are: *Am I getting data from everything I should (How many devices are sending events)? Is the right data being collected (Are all data logs the correct ones)?* Another item to track is how often mobile devices are switched out, which is much more frequent than laptops. It is possible to find user accounts with multiple devices attributed to them, and IT administrators will need to determine if it is a new device or a compromised account.

Table 4.3.8-1

Control 8: Audit Log Management				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
8.1	Network	Protect	Establish and Maintain an Audit Log Management Process	•	•	•	Y	IT professionals should understand the types of logs available to them with their organization's unique combination of mobile devices, infrastructure, and mobile apps.
8.2	Network	Detect	Collect Audit Logs	•	•	•	Y	Audit logs can often be obtained via a UEM, EMM, or MDM interface. Logs can also be obtained by forcing all traffic through a UEM's VPN tunnel to the corporate network.
8.3	Network	Protect	Ensure Adequate Audit Log Storage	•	•	•	Y	This is always a concern for any type of Information system log collection application.
8.4	Network	Protect	Standardize Time Synchronization		•	•	N	iOS and Android devices primarily utilize the cellular network (potentially via the Network Identity and Time Sone (NITS) protocol) or the GPS network for their source of time. Within the mobile OS, they can generally only be synced to a single time source via the Network Time Protocol (NTP). Developers may be able to design individual applications to utilize additional time sources.
8.5	Network	Detect	Collect Detailed Audit Logs		•	•	Y	This is always a concern for any type of Information system.
8.6	Network	Detect	Collect DNS Query Audit Logs		•	•	N	There is nothing specific to mobile within this Safeguard, although mobile devices can be configured to use a specific DNS server which would facilitate logging the queries.
8.7	Network	Detect	Collect URL Request Audit Logs		•	•	N	There is nothing specific to mobile within this Safeguard.
8.8	Devices	Detect	Collect Command-Line Audit Logs		•	•	N	Unless devices are jailbroken or rooted, this is generally not a concern on mobile devices.
8.9	Network	Detect	Centralize Audit Logs		•	•	Y	Audit logs can often be obtained via an EMM or MDM interface.
8.10	Network	Protect	Retain Audit Logs		•	•	N	Not Applicable
8.11	Network	Detect	Conduct Audit Log Reviews		•	•	Y	Administrators and IT professionals should review audit logs for unexpected accesses to enterprise resources and other detection opportunities relevant to their mobile deployment.
8.12	Data	Detect	Collect Service Provider Logs			•	Y	If this information is available, it should be collected and analysed.

4.3.9 CONTROL 09 Email and Web Browser Protections

Mobile Applicability

Traditional email gateway security controls for reducing spam, phishing attacks, malware, and malicious URL links all apply to mobile. Mobile devices change the traditional enterprise architecture by not only extending it outside a traditional perimeter, but also bypassing the need to route much or all traffic through the enterprise network due to use of cloud services. However, web and email threats are still a concern with mobile devices. Additionally, MTD can apply host-based protection via an on-device VPN interface and review all links and pages visited.

Mobile Deployment Considerations

In situations where a full-device (or on-demand) VPN is not in use, a reverse proxy might be useful to act as a centralized, authenticated access point to corporate data and resources, with the added benefit that the access point can be controlled (turned on or off) based on device compliance policies. Organizations may wish to utilize additional agent-based tools with devices that are not provisioned into an EMM. This does assist with compartmentalization, and many of the MDM / MAM tools provide their email and web apps with a corresponding proxy service. This is not required, but many organizations choose to use it.

It is important to point out, however, that from a usability perspective and an update perspective, it is often preferable to utilize the native solutions that are available. There is often a period of time when a new version of a mobile OS is released and subsequently installed, and the third-party email and browser apps are not updated and do not function as intended. Several MTD solutions include phishing protection capabilities that can be implemented in different ways based on the MTD solution's design.

Mobile Additional Discussion

An on-device approach provides a better view into the threats affecting an employee's use of email and web browsers. This includes malicious applications, profiles, and network attacks (e.g. man-in-the-middle web proxy attacks). Some tools use on-device visibility to analyse sites that can be serving up malware or attempting to phish the user to collect credentials. There are also tools and approaches that funnel mobile traffic through filtering cloud infrastructures that perform web gateway filtering and security functions. Bandwidth, performance, and usability concerns should be considered and funnelling all traffic back to the corporate network for inspection should generally be avoided.

Mobile security providers often provide dedicated email clients and browsers for employees to use with their corporate email that the vendor and organization can have additional control over. These clients and browsers may be internally developed, or utilize important libraries and kits from other on-device browsers. At the very least, these alternative applications will run under a different user and application ID, providing additional protections to isolate a user's personal and corporate email. Regardless, all email clients and browsers should be obtained from an authorized repository, written by a trustworthy developer, and kept up-to-date in order to remain effective.

Table 4.3.9-1

Control 9: Email and Web Browser Protections				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
9.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	•	•	•	Y	Browsers and email clients should be kept up-to-date. This is especially important if an organization is wrapping the app or using a custom app that cannot be updated via the normal mobile application store update process that a user would be familiar with. Of note, Android and iOS provide apps with their browser capability in most cases via APIs to deploy webviews: the rendering of http(s) delivered content. This is the typical implementation for an application. This common process makes this Safeguard very important.
9.2	Network	Protect	Use DNS Filtering Services	•	•	•	Y	Use DNS filtering services on all end-user devices, including remote and on-premises assets, to block access to known malicious domains. This ensures that end-user devices have DNS filtering enabled as a means of providing additional protection above that traditionally offered by URL filtering services.
9.3	Network	Protect	Maintain and Enforce Network-Based URL Filters		•	•	Y	Network-based proxies, firewalls, and other proxies can be configured for mobile devices, or specifically support capabilities to filter mobile traffic. Content blockers can be developed for certain applications. A mobile VPN can also force mobile traffic requests through an enterprise managed URL filter.
9.4	Applications	Protect	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		•	•	N	Email client and browser plugins generally do not exist for the mobile versions of these applications.
9.5	Network	Protect	Implement DMARC		•	•	N	Although DMARC is important, there is nothing to be done specifically for mobile within this Safeguard.
9.6	Network	Protect	Block Unnecessary File Types		•	•	Y	This can be performed via an EMM's email security policies.
9.7	Network	Protect	Deploy and Maintain Email Server Anti-Malware Protections			•	N	Although an important Safeguard, there is nothing specific to mobile. A large percentage of mobile malware is delivered via a chatting app (e.g. SMS, Messenger), which may not be in the path of enterprise filtering solutions.

4.3.10 CONTROL 10 Malware Defences

Mobile Applicability

Mobile malware primarily takes the form of malicious applications, updates to legitimate applications to deliver malicious capability, and browser-based malware. Another example threat vector for malware is via Android Debug Bridge (ADB) that can be exposed via Universal Serial Bus (USB) debugging capabilities and remotely accessible via port 5555. That is not to say that hardware and firmware vulnerabilities do not exist and are exploited, but the vast majority of mobile malware takes the form of malicious applications. Mobile malware utilizes track patterns that are different from traditional desktop-based malware, such as tricking a user into accepting a management profile, and differences even exist between the mobile operating systems. Some widely-used mobile OS vendors have defined an entire system of classifying mobile malware that have been regularly updated.

A large majority of mobile malware is targeted at Android devices. The delivery of Android malware is usually via a form of social engineering intended to get the user to install a seemingly legitimate app. Another related attack vector is when the user searches for an app online rather than via the commonly-used mobile operating system app stores. For example, iOS malware delivery takes two primary forms when it does exist because the application restriction with digital code signing requirements from Apple render most malicious applications very difficult to run on the device. SMS or chat message delivery of a link to a website which contains exploit code designed specifically for iOS is one rarely observed, but an observed exploitation strategy. The second is delivery via enterprise-signed applications. This minor exception to the digital signature requirement is the most commonly used method by malware authors. They purchase an enterprising signing app from Apple, then use it to digitally sign the application. This code, unlike the code available in the apps in Apple's store, is never reviewed by Apple. Unless users report the digital signature for delivering malicious code, no one would know and the malware campaign could proceed. The only defence is the user should choose to accept the enterprise certificate profile. This is the case where user training is important on a simple behaviour: *only install applications from authorized application stores*.

Mobile Deployment Considerations

The proper configuration settings on mobile devices can help to mitigate a large percentage of mobile malware, such as ensuring the mobile sandbox is intact and being enforced. These configurations should be enforced to the degree possible before users are provided a device. The same goes for updating the mobile OS:

- **BYOD:** From a BYOD perspective, personal phones are a greater risk, as users download a larger number of apps for personal use than business use. Users should be educated about their role preventing the installation of malware. One of the most important malware defences possible on mobile is preventing employees from using an unofficial app store. *"Devices and data can be at increased risk when such apps are installed from unverified sources"*.
- **Fully-managed:** The configurations of fully-managed devices can be mandated and enforced, which lessens the risk of malware accidentally being installed on the device. Use of MTD can be mandated without the user's ability to turn it off, and the MTD application can receive regular updates. Use of native app stores, or enterprise app stores, can be enforced.

Mobile Additional Discussion

Traditional anti-malware techniques are not feasible on iOS, due to the platform not allowing access at a level where applications can have general knowledge about other applications running on the device. This does not apply to jailbroken and rooted devices, which are particularly susceptible to malware and general attacks. MTD host-based agents can provide anti-malware protection, especially if they are provided a privileged access via an EMM or profile / admin access. Another technique is to review mobile applications off-device and then match hashes of the apps installed on the device against that analysis. This type of application vetting process is detailed within NIST SP 800-163 [i.21].

Another product category that is helpful is mobile threat intelligence. These services review apps and provide a risk rating or threat score based on app capabilities, behaviour, and other analysis, to mobile administrators. The information can be used to help make the installation decision easier for both admins and end users. Mobile app vetting tools can also serve a similar function by performing static and dynamic analysis to find vulnerabilities and identify Trojan apps. Many of the tools described within this clause may be able to integrate with EMMs so that one dashboard can be used.

Finally, mobile devices themselves are also risks to Personal Computers (PCs). Email attachments forwarded from mobile devices might have PC malware that does not affect the mobile device, but could infect the PC. Mobile devices connected via USB to a PC could also have malicious PC files, as they can act as removable media. Traditional PC antivirus also cannot always scan mobile devices like a traditional USB drive. Traditional PC USB port monitoring can help with the threat of a mobile device connected to a PC.

Table 4.3.10-1

Control 10: Malware Defenses				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
10.1	Devices	Protect	Deploy and Maintain Anti-Malware Software	•	•	•	Y	In the context of mobile, mobile threat defence is the common technology used to detect malware.
10.2	Devices	Protect	Configure Automatic Anti-Malware Signature Updates	•	•	•	Y	MTD applications should be kept up-to date with their subscriptions active.
10.3	Devices	Protect	Disable Autorun and Autoplay for Removable Media	•	•	•	N	Mobile devices can be configured to prevent specific applications from running once a device is newly booted. Yet, mobile apps generally do not autoplay when a peripheral is plugged into the device, although a notification may be presented to the user prompting the user to manually open the app. Note that Android can granularly define what functions can be performed over physical USB connectivity (e.g. file sharing, power).
10.4	Devices	Detect	Configure Automatic Anti-Malware Scanning of Removable Media		•	•	N	Removable devices generally are not supported on mobile devices, and MTD apps would not have access to them.
10.5	Devices	Protect	Enable Anti-Exploitation Features		•	•	N	These are enabled by default on modern versions of mobile operating systems.
10.6	Devices	Protect	Centrally Manage Anti-Malware Software		•	•	Y	This would often be through the usage of an MTD product, although some EMMs and mobile threat intelligence server-side applications also contain this capability.
10.7	Devices	Detect	Use Behaviour-Based Anti-Malware Software		•	•	Y	MTD monitors the behaviour of mobile apps on a mobile device.

4.3.11 CONTROL 11 Data Recovery

Mobile Applicability

Mobile devices are designed to make data available to users in a manner as easy as possible, and this includes backing data up. The two major mobile platforms have their own ecosystems to alleviate backup concerns that can often be used via a few configuration options. Many organizations find it more of a worry to have enterprise information unintentionally stored on unapproved servers and systems. The native backup utilities primarily attempt to back up a user's contacts, photos, text messages, and documents. These are stored in the mobile OS supporting platform(s), such as iCloud. Accordingly, only certain file formats and data storage locations can be backed up. Beyond this, certain applications have their own cloud storage methods and platforms to assist with data recovery, but they should be appropriately configured before they should be considered sufficiently reliable for enterprise usage. Mobile applications can configure which files and hardware stored data (such as the keychain on iOS) is permitted to be backed up or excluded from backup. Application developers who are creating organization-specific applications should prevent backup of sensitive files and tokens. Similarly, third-party applications used for enterprise purposes should be reviewed for backup strategies for sensitive data.

Mobile Deployment Considerations

This Control applies regardless of deployment scenario. This Control is easier to accomplish with a fully-managed or COPE device since data stays in the work container. Utilizing cloud apps is also an effective strategy since all data can reside in a cloud platform. Special considerations should be taken in BYOD and shared-device situations to prevent sensitive user data, such as photos, from being backed up and intermingled with enterprise data. This requires both the enterprise and user working together toward this common goal, necessitating additional user education. On the other side of the coin, when an enterprise needs to wipe a device for whatever reason, any enterprise information needs to have already been backed up onto an approved storage location, in order to enable a data restore to another device.

Mobile Additional Discussion

Organizations should verify and review backup (e.g. iCloud, Google) settings to make sure the proper information is backed up and encrypted, and that improper information is not backed up. This might include corporate email, corporate contacts or calendar, or documents (e.g. xlsx, docx, pdf) to personal backup. The former would generally be stored on the corporate Exchange server already with mobile devices fetching that information as needed. Corporate policies should be specified for backing up enterprise data to a public cloud - especially if it is not a cloud platform or service provided and approved for corporate usage by the organization. Proper authentication mechanisms and other controls should be in place to protect any enterprise cloud backup.

Mobile devices may also intentionally or unintentionally back up information to any desktop environment they are physically or wirelessly connected to. The creation of these backups should be prevented unless specifically authorized by the enterprise. Desktop backups should also be protected via an authentication mechanism and cryptographic means.

Table 4.3.11-1

Control 11: Data Recovery				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
11.1	Data	Recover	Establish and Maintain a Data Recovery Process	•	•	•	Y	Organizations should document the processes used to back up and also recover enterprise information on mobile.
11.2	Data	Recover	Perform Automated Backups	•	•	•	Y	Users should regularly back up enterprise data to approved backup locations. Enterprises should provide guidance for how to configure the mobile OS and applications to accomplish this goal. Automated backups are not always possible on mobile. Automated backup is most commonly in the form of synchronization to cloud resources on mobile.
11.3	Data	Protect	Protect Recovery Data	•	•	•	Y	Some cloud-based services will do this automatically, but users and enterprises need to check on the mitigations in place before electing to use a service, such as multifactor authentication. Any removable media for the device, alongside desktop backups, also needs to be protected.
11.4	Data	Recover	Establish and Maintain an Isolated Instance of Recovery Data	•	•	•	Y	Ransomware and its variants (e.g. destructive malware) typically perform malicious activities on-device. In mobile scenarios, this type of malware typically prevents a user's access to the device. Similar to traditional scenarios, enterprise information should be regularly backed up offline to prevent this type of attack from being successful.
11.5	Data	Recover	Test Data Recovery		•	•	Y	Employees and administrators should regularly perform this action. An easy way of testing this is going through the motions of provisioning a new phone or application to a new device.

4.3.12 CONTROL 12 Network Infrastructure Management

Mobile Applicability

This clause has little direct effect on mobile security and more generally applies to the secure usage of network devices. Guidance on Wi-Fi security is available and applicable in this situation, but that guidance applies to all computing devices utilizing Wi-Fi.

Mobile Deployment Considerations

Mobile deployment models do not have an impact on this Control. This Control primarily protects the servers and network devices that mobile devices leverage for enterprise access.

Mobile Additional Discussion

It is uncommon, although not impossible, for organizations to have devices specific to mobile devices in their network. Examples include VPN concatenators specific to mobile, and any telecommunications equipment the organization may own.

Note that this Control is not meant for telecommunications companies operating large, interconnected networks.

Table 4.3.12-1

Control 12: Network Infrastructure Management				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
12.1	Network	Protect	Ensure Network Infrastructure is Up-to-Date	•	•	•	N	Not Applicable.
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		•	•	N	Not Applicable.
12.3	Network	Protect	Securely Manage Network Infrastructure		•	•	N	Not Applicable.
12.4	Network	Identify	Establish and Maintain Architecture Diagram(s)		•	•	N	Not Applicable.
12.5	Network	Protect	Centralize Network Authentication, Authorization, and Auditing (AAA)		•	•	N	Not Applicable.
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		•	•	N	Not Applicable.
12.7	Devices	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		•	•	N	Not Applicable.
12.8	Devices	Protect	Establish and Maintain Dedicated Computing Resources for All Administrative Work			•	N	Not Applicable.

4.3.13 CONTROL 13 Network Monitoring and Defence

Mobile Applicability

Mobile devices remove the concept of the traditional infrastructure boundary by allowing users to work completely locally, or frequently accessing cloud-based services directly, without routing through corporate infrastructure. With this in mind, a subset of traditional boundary defence concepts can still apply to mobile devices. Traditional network monitoring tools, email security, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) alerts, logging of events and alerts, and VPNs all remain important. Many of the Safeguards in this Control do not apply since they are focused on network configurations or provide protections from outside of the mobile devices.

Architectural decisions from the enterprise will decide if many of these Safeguards are implemented directly into the enterprise or via some components hosted in the cloud. In one scenario, device traffic can be routed through the enterprise, while in the other scenario, traffic can be sent through cloud infrastructure. Many enterprises will use a combination of these two approaches, as some important services are only available via third-party cloud platforms.

Mobile Deployment Considerations

Enterprises should keep in mind that most mobile devices are explicitly outside of the network boundary, regardless of deployment scenario. A mobile device is a network endpoint when it is physically inside a corporate facility connecting via Wi-Fi, as it is when a local or remote device is utilizing an always-on VPN. When a device is solely accessing information without a VPN, it is not considered a network endpoint. Even with an always-on VPN obtaining an internal IP address, certain types of traffic will not be sent through the enterprise VPN. Examples include diagnostic information about the device, OS traffic communication with an ecosystem provider, Wi-Fi, Bluetooth, and cellular traffic. The device ultimately leaks information to any malicious actors passively sniffing this information and can help attackers fingerprint the device. In part because of this, BYOD scenarios should have additional security controls implemented on the device, and perhaps also on the home network of the user:

- **BYOD:** These devices can leverage MTD applications to be made aware of a subset of network-based attacks. MTD applications often lack the permissions or APIs to defend devices in a similar manner to host-based IDPS devices. BYOD devices can also leverage a VPN application to connect to the enterprise.
- **Fully-managed:** These devices can also be outfitted with MTD applications. Fully-managed devices can also leverage a VPN application to connect to the enterprise. Enhanced forms of authentication can be achieved in the fully-managed scenarios as digital certificates can be provisioned to the device.

Mobile Additional Discussion

Organizations should choose to utilize a VPN for all BYOD or remote devices. Where the VPN is terminated within the network is a choice for the enterprise, based on security concerns and policy / legal considerations. However, there are also tools and approaches that funnel mobile traffic through filtering cloud infrastructures that perform web gateway filtering and security functions.

Devices will usually automatically attempt to access Wi-Fi networks they have previously been associated with and connected to. If the option to refrain from automatically connecting is available, users should be encouraged to select it. Blacklisting certain Service Set Identifiers (SSIDs) on devices, such as those from major retailers and cafes, can help prevent a user's device from accessing a rogue version of that network and sending sensitive enterprise data over it. Some mobile devices will automatically enable Wi-Fi based on previously connecting in that location. Also, some devices use Wi-Fi for geolocation using Wi-Fi even if the Wi-Fi connection is disabled. The privacy exposure this might cause is frequently addressed by using a random MAC address for the Wi-Fi card.

Table 4.3.13-1

Control 13: Network Monitoring and Defense				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
13.1	Network	Detect	Centralize Security Event Alerting		•	•	Y	Administrators can use a SIEM to correlate security events from mobile devices with other events occurring in the enterprise network.
13.2	Devices	Detect	Deploy a Host-Based Intrusion Detection Solution		•	•	Y	MTD technologies fill this niche on mobile.
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution		•	•	N	Enterprises can ensure that any relevant IDS is "mobile aware". This Safeguard is better and more easily enforced when devices are taking advantage of a VPN.
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments		•	•	Y	Mobile devices obtaining an IP on the internal network often come from a separate pool of IP addresses dedicated to these devices.
13.5	Devices	Protect	Manage Access Control for Remote Assets		•	•	Y	Administrators should have some degree of control over the security and configuration of any mobile devices accessing an internal network, if this is needed at all.
13.6	Network	Detect	Collect Network Traffic Flow Logs		•	•	N	Although a useful Safeguard, there is nothing specific to mobile.
13.7	Devices	Protect	Deploy a Host-Based Intrusion Prevention Solution			•	Y	MTD technologies fill this niche on mobile, although their ability to "prevent" vs. "detect" is much lower on mobile.
13.8	Network	Protect	Deploy a Network Intrusion Prevention Solution			•	N	Enterprises can ensure that any relevant IPS is "mobile aware". This Safeguard is better and more easily enforced when devices are taking advantage of a VPN.
13.9	Devices	Protect	Deploy Port-Level Access Control			•	Y	Widely-used mobile operating systems support port level access control.
13.10	Network	Protect	Perform Application Layer Filtering			•	N	Although this Safeguard is quite useful, there is nothing specific to mobile about it.
13.11	Network	Detect	Tune Security Event Alerting Thresholds			•	N	Although this Safeguard is quite useful, there is nothing specific to mobile about it.

4.3.14 CONTROL 14 Security Awareness and Skills Training

Mobile Applicability

Users and administrators should be trained on risks and threats specific to mobile platforms. Security awareness training can be tailored to remote employees, contractors, and all employees accessing corporate email using mobile devices.

Mobile Deployment Considerations

Remote employees, and those using devices in a BYOD mobile deployment scenario, should be provided security awareness training dedicated to the threats most affecting BYOD. This includes device loss and theft, data loss via malicious applications, Application Data (AD) credential theft via phishing, and the mixing of personal / enterprise information. More traditional mobile deployment scenarios are also at risk, but BYOD should be given additional time and consideration, with the importance of these issues impressed upon the employee:

- BYOD: No installation of applications from unofficial app stores; scepticism of all messages and URLs; minimize installation of applications, uninstalling or disabling anything that is unused; minimize permissions granted to apps, limiting location, voice, and camera use to while the app is in the foreground only.
- Fully-managed: same, plus maintaining appropriate separation of personal activities not on the managed asset.

Mobile Additional Discussion

Many of the risks and threats affecting mobile users require direct user interaction in order to be mitigated - even if there is an MDM or enterprise administrator managing the device. The large majority of Safeguards applicable to mobile that are not technically implementable are candidates for security awareness training. Candidates include Controls 4 (Secure Configuration of Enterprise Assets and Software) and 9 (Email and Web Browser Protections). Many of these Controls are not necessarily for mobile devices, but are infrastructure components that enable secure usage. Additional items include enterprise policies surrounding trustworthy replaceable components (e.g. digitizer, screen, battery). For instance, devices accessing enterprise information should not be replaced by an untrustworthy technician as they will have unsupervised physical access with the device and may install malicious components / software.

Security awareness training for mobile should at first focus on lock screen security and the prevention or mitigation of device loss / theft. Additionally, serious focus should be provided for SMS phishing and various ways that users can be tricked into clicking on dangerous links or installing Trojan mobile apps that will steal passwords. Subscriber Identity Module (SIM) swapping can also be a dangerous social engineering technique that can affect an enterprise that users should be aware of. Employees should be trained against these types of attacks via regularly scheduled white hat phishing and chat / SMS messaging campaigns that are specific to mobile social engineering scenarios.

Table 4.3.14-1

Control 14: Security Awareness and Skills Training				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
14.1	N/A	Protect	Establish and Maintain a Security Awareness Program	•	•	•	Y	A holistic, long-term approach should be developed to address user education concerns surrounding the use of mobile.
14.2	N/A	Protect	Train Workforce Members to Recognize Social Engineering Attacks	•	•	•	Y	Pre-texting by phone is common and can be used to obtain information about the mobile devices and applications used by the enterprise.
14.3	N/A	Protect	Train Workforce Members on Authentication Best Practices	•	•	•	Y	Secure authentication is different on mobile platforms and employees should know the security risks and implications of using SMS as a second factor. This method of authentication is no longer supported by NIST for U.S. agencies.
14.4	N/A	Protect	Train Workforce on Data Handling Best Practices	•	•	•	Y	Users should understand what data is sensitive on their mobile devices and how to prevent commingling alongside personal information.
14.5	N/A	Protect	Train Workforce Members on Causes of Unintentional Data Exposure	•	•	•	Y	This can be tailored to mobile-specific causes such as installing insecure apps on corporate devices or forgoing multifactor authentication. This can also be a result of lost device, or granting access to the device to an unauthorized person.
14.6	N/A	Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	•	•	•	Y	Employees can be trained on what successful attacks on mobile devices look like, and to whom they should be reported.
14.7	N/A	Protect	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	•	•	•	Y	This Safeguard can be tailored to users learning how to ensure apps and devices are up-to-date.
14.8	N/A	Protect	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	•	•	•	Y	Employees should be trained on how to securely access enterprise resources given the tools provided by the enterprise.
14.9	N/A	Protect	Conduct Role-Specific Security Awareness and Skills Training		•	•	Y	Role-specific awareness training should include a mobile component. Training for the risks of mobile should be provided to the system administrators responsible and sponsors of the mobile deployment.

4.3.15 CONTROL 15 Service Provider Management

Mobile Applicability

The primary service providers for mobile devices include the EMM / MDM provider, alongside companies offering MTD, MAM, VPN, and mobile app development technologies. Organizations may wish to group their mobile network operator, device manufacturer, or mobile operating system developer as a service provider. While this is reasonable, small to medium businesses may be unable to ensure these large companies implement many of the practices necessitated by the Safeguards found within this Control.

Mobile Deployment Considerations

The mobile device deployment model an organization chooses to use will dictate which service providers are required. With that said, there are few differences for the Safeguards put onto BYOD versus fully-managed devices in this Control. Instead, one of the main decisions that affect security in this Control is if mobile data is stored on-premises or primarily hosted in cloud services. Cloud-based service providers offering mobile services will regularly be hosting and interacting with enterprise mobile data. In reality, many organizations will have a hybrid approach, utilizing both on-prem and cloud services. Cloud-based service providers will have direct access to the data and the enterprise should ensure security requirements are in place before usage to properly safeguard their data in the cloud.

Mobile Additional Discussion

This Control revolves around obtaining assurances from service providers as to their cybersecurity practices. Not all service providers will protect an organization's data in the same manner. Accordingly, a service provider's cybersecurity posture affects their ability to safeguard enterprise data entrusted to them.

Table 4.3.15-1

Control 15: Service Provider Management				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
15.1		Identify	Establish and Maintain an Inventory of Service Providers	•	•	•	Y	The primary service providers for mobile devices include the EMM / MDM provider, alongside companies offering MTD, MAM, VPN, mobile threat intelligence, and mobile app development technologies.
15.2		Identify	Establish and Maintain a Service Provider Management Policy		•	•	Y	Policies for working with service providers should address handling enterprise data generated by, and traditionally stored on, mobile devices. Updates to this policy may be necessary when major changes happen to mobile devices, such as the addition of new functions via a major OS update.
15.3		Identify	Classify Service Providers		•	•	Y	Email, contacts, and calendar, alongside text messages, are often the most valuable information stored on mobile devices. The enterprise resources they can access are often also sensitive. Service providers should be classified based on the sensitivity of mobile data and enterprise functions they can access and/or host.
15.4		Protect	Ensure Service Provider Contracts Include Security Requirements		•	•	Y	Service providers offering mobile services should also adhere to the security requirements of the enterprise. Security requirements for mobile devices are most effective when specifically developed for mobile devices (e.g. NIST SP 800-124 [i.19]).
15.5		Identify	Assess Service Providers			•	Y	Obtaining evidence of adherence to security requirements for mobile service providers should be done in a similar manner to other service providers leveraged by the enterprise.
15.6	Data	Detect	Monitor Service Providers			•	Y	Monitoring mobile service providers should be done in a similar manner to other service providers leveraged by the enterprise.
15.7	Data	Protect	Securely Decommission Service Providers			•	Y	Enterprises need to ensure mobile service providers are securely decommissioned, to remove any data saved in their system to include user accounts, passwords, and credentials.

4.3.16 CONTROL 16 Application Software Security

Mobile Applicability

The security of individual mobile applications is important, as millions of apps are freely available for personal and business use. These apps may reside within official public app stores, unofficial public stores, or private app stores / repos hosted by enterprises. App stores hosted by an organization are often referred to as *private app stores* or *enterprise app stores*. These private app stores are often used to host apps that are developed in-house and are not available to the general public. Secure software development is a complex process that has unique considerations for mobile. Once apps are developed, they typically go through a process known as "mobile app vetting" to analyse the security of an app. The tools, procedures, and testing processes for engaging in application security for mobile apps is generally different from applications developed for laptops and server environments.

Mobile Deployment Considerations

It is more difficult to ensure that properly vetted apps are running on unmanaged devices. Fully-managed devices can whitelist apps and prevent the installation of unwanted ones. Managed devices can have profiles that sign privately developed apps, allowing them to bypass the restrictions of the primary app stores. This potentially provides additional functionality and usage of private or sensitive APIs:

- BYOD: This Control does not lend itself to deployment-specific recommendations.
- Fully-managed: This Control does not lend itself to deployment-specific recommendations.

Mobile Additional Discussion

Mobile apps may leverage web technologies in whole or part or may solely leverage the mobile frameworks provided by the OS. Web technologies are not the only external technologies that may be utilized to develop mobile apps. Third-party mobile libraries, Software Development Kits (SDKs), and libraries created for more traditional server and enterprise use cases may be embedded into mobile apps. Mobile application vetting can help to identify if there are discrete software vulnerabilities that can be exploited within any of the technologies used within the application. Additionally, unintentional dangerous behaviour and malware embedded into the application can be found. Examples of mobile application risks include accessing sensitive personal information (e.g. text messages, photos, contacts), accessing sensitive enterprise information, or directly attacking the underlying operating system and firmware. Malicious native apps have also been seen to be turning on the camera or microphone, logging geolocation, capturing credentials, initiating toll calls or texts, or creating nuisance issues like resource saturation that drains the battery.

Additional resources can be found in the Bibliography references.

It is extremely important to ensure that users are installing legitimate versions of an app, and that those apps are up-to-date. Trojan and repackaged apps are some of the most pernicious and successful types of malware in widely-used operating system play stores.

Table 4.3.16-1

Control 16: Application Software Security				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process		•	•	Y	In the context of mobile, establishing a secure software development process is focused on mobile applications often developed internally or external software development companies. See Bibliography references.
16.2	Applications	Protect	Establish and Maintain a Process to Accept and Address Software Vulnerabilities		•	•	Y	A vulnerability disclosure policy is key for receiving reports of vulnerabilities in an enterprise's own software and addressing them before they are able to be publicly exploited. Vulnerability disclosure policies should include mobile apps and procedures to quickly remedy vulnerabilities.
16.3	Applications	Protect	Perform Root Cause Analysis on Security Vulnerabilities		•	•	Y	This is an important step to ensure that vulnerabilities of the same type do not repeatedly occur in an organization's codebase.
16.4	Applications	Protect	Establish and Manage an Inventory of Third-Party Software Components		•	•	Y	Third-party libraries, frameworks, and other technologies leveraged by mobile app developers should be identified, understood, and inventoried.
16.5	Applications	Protect	Use Up-to-Date and Trusted Third-Party Software Components		•	•	Y	Inventoried third-party mobile components should be regularly reviewed for support, and updated.
16.6	Applications	Protect	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities		•	•	Y	Administrators and security professionals will benefit from rating mobile device vulnerabilities. The Common Vulnerability Scoring System (CVSS) [i.20] does not differentiate between system types and is applicable to mobile devices and their associated management systems. A list of objectionable app behaviours unique to each enterprise can be compiled. For example, collecting all contacts and moving to the application's infrastructure may be considered objectionable (while still technically permitted by the OS permissions for apps) particularly important to an enterprise. Apps exhibiting this behaviour can then not be accepted for use.
16.7	Applications	Protect	Use Standard Hardening Configuration Templates for Application Infrastructure		•	•	N	These templates are typically unavailable for mobile.

Control 16: Application Software Security				Implementation Groups			Applicability	
16.8	Applications	Protect	Separate Production and Non-Production Systems		•	•	Y	Establish and maintain separate mobile development and production environments. Non-production apps should not be exposed to production infrastructure, as they commonly store sensitive data, but are often not hardened or running up-to-date software.
16.9	Applications	Protect	Train Developers in Application Security Concepts and Secure Coding		•	•	Y	Classes and training materials are easily available online and in-person to educate developers on the common pitfalls of secure software development for mobile platforms.
16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures		•	•	Y	Classes and training materials are easily available online and in-person to educate developers on the common pitfalls of secure software development for mobile platforms.
16.11	Applications	Protect	Leverage Vetted Modules or Services for Application Security Components		•	•	Y	Mobile app developers should leverage vetted security technologies whenever possible in lieu of building their own. Examples include secure containers, identity management, and mobile threat detection.
16.12	Applications	Protect	Implement Code-Level Security Checks			•	Y	Static and dynamic analysis tools dedicated to mobile devices are available. In many cases, the mobile app is uploaded to a service, and a report back is received. On-premises solutions exist for both static code and dynamic runtime testing.
16.13	Applications	Protect	Conduct Application Penetration Testing			•	Y	Firms exist that specialize in mobile app penetration testing.
16.14	Applications	Protect	Conduct Threat Modelling			•	Y	Threat modelling should be conducted for mobile devices. NIST SP 800-124 [i.19] can assist in mobile threat modelling, as can references in Bibliography.

4.3.17 CONTROL 17 Incident Response Management

Mobile Applicability

Traditional Incident Response (IR) guidance applies, most of which can be tailored to mobile. This includes the need for planning, defining roles and responsibilities, and identifying escalation paths. Now that many users access company data and services with mobile devices in a manner similar to PCs, the need to identify, investigate, respond, and recover from incidents involving mobile devices is important. A mobile incident response plan is sometimes separate from the normal plan, but many times it is folded into an organization's overall strategy.

Common scenarios which should be planned for: lost / stolen device, if a remote wipe of a lost / stolen device was not successful, suspicion of mobile malware, suspicion of "spouse tracker" style eavesdropping / privacy invading malicious software, malicious phishing / SMS / chat link sent, foreign travel planning, and post-travel inspection.

Mobile Deployment Considerations

By utilizing UEM for any deployment scenario, IR can be more effective for mobile, such as by remote wiping a work container. Significant challenges exist for incident response activities associated with BYOD devices. Incident response activities can severely affect an employee's or contractor's personal privacy. An individual's mobile phone can be considered an intimate part of their life, as the personal data stored within is quite sensitive. Individuals often have their entire digital life on their phones, from texts, calendar, contacts, and photos. Reverse-engineering the path someone's taken in the world is possible via the geolocation metadata from pictures, social networking check-ins, and applications that store a person's "last active location". It is also possible to reveal someone's personal contact network via phone logs, text messages, email, and private social network accounts.

Mobile Additional Discussion

Operations personnel and incident responders need to be trained on what to look for with unusual behaviour on the mobile devices. For example, if a user receives hundreds of messages around the same time from an account or application on the device, it is often a sign that a service or device has been compromised. A major challenge in mobile response and recovery activities is the vast quantity of different types of mobile device hardware, even among generations of products. When considering data forensics for mobile devices, a wealth of different types of data is available to support the objective of the acquisition, be it eDiscovery, misuse, or evidence collection to support a criminal case.

For more information see Bibliography references.

Table 4.3.17-1

Control 17: Incident Response Management				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
17.1		Respond	Designate Personnel to Manage Incident Handling	•	•	•	Y	Appropriate staff-level and management personnel should be specifically appointed for mobile incident response.
17.2		Respond	Establish and Maintain Contact Information for Reporting Security Incidents	•	•	•	Y	Information for specific individuals and external organizations should be maintained for those who should be contacted regarding mobile security incidents.
17.3		Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	•	•	•	Y	Information regarding mobile breaches and other incidents should be made available to internal employees per established processes. This information can be fed back into awareness training.
17.4		Respond	Establish and Maintain an Incident Response Process		•	•	Y	Written plans for EMM and mobile device breaches are key to mobile incident response.
17.5		Respond	Assign Key Roles and Responsibilities		•	•	Y	Especially if an enterprise is supporting a mobile application, personnel should be dedicated to mobile IR and understand the fundamentals of EMM, iOS, and Android.
17.6		Respond	Define Mechanisms for Communicating During Incident Response		•	•	Y	Processes for reporting mobile incidents should be put in place that are mandated across the enterprise. This should include the time to report, types of anomalous events, and the details of any relevant mobile incident.
17.7		Recover	Conduct Routine Incident Response Exercises		•	•	Y	Breaches of mobile apps and management systems can be periodically assessed in order to test mobile incident response procedures. This also helps to keep the necessary individuals aware of the mobile IR procedures.
17.8		Recover	Conduct Post-Incident Reviews		•	•	Y	Make sure to interview personnel involved in mobile IR in order to ensure all necessary actions are performed, and procedures are updated to include any new areas not initially envisioned.
17.9		Recover	Establish and Maintain Security Incident Thresholds			•	Y	Depending on their criticality to the organization, a security incident affecting mobile systems may be more or less important to the enterprise.

4.3.18 CONTROL 18 Penetration Testing

Mobile Applicability

Traditional penetration testing and Red Team activities, such as running scans to see which ports are open, and what vulnerable services they are supporting, does not apply. However, penetration testing of mobile deployments is an important and worthwhile activity. The use of mobile generally expands the attack surface of an organization, making additional methods available to attackers for social engineering and technical attacks on devices and apps. For instance, SIM swapping or an SS7-based attack is applicable to mobile devices but not most other types of systems.

Mobile Deployment Considerations

Penetration testers and Red Team members should pay extra care in securing authorization to perform vulnerability assessment and penetration testing activities on BYOD devices. Specific user approval may be necessary in addition to any authorization to what is typically provided by the enterprise. Accidentally deleting a user's personal data or bricking their mobile device could cause contractual and legal difficulties. The better approach is to simulate the scenarios of use by users with representative mobile devices and applications.

Mobile Additional Discussion

Many of the attack techniques discussed throughout the present document, such as sniffing mobile traffic over the air and man-in-the-middle attacks, are possible. However, interception of traffic sent over 3G/4G/5G networks is impractical for most organizations. When testing mobile device network communications, use of Wi-Fi networks inspection or on-device capture is the most practical approach. Widely-used mobile operating systems provide available tools.

Potentially the most vulnerable portions of your mobile deployment may be the mobile apps themselves. The traditional approach for mobile app testing has been code review tools, but standard web proxy tools and web application penetration testing techniques are possible and should be explored. Use of an experimental lab and test devices for more thorough hardware examination is also relevant to mobile. See Bibliography for penetration testing resources.

Table 4.3.18-1

Control 18: Penetration Testing				Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.10] for description)	IG1	IG2	IG3	Included?	Justification
18.1		Identify	Establish and Maintain a Penetration Testing Program		•	•	Y	A penetration testing program focused on mobile systems will include any relevant mobile applications, mobile devices, where possible, network interception strategies used by adversaries, and management infrastructure.
18.2	Network	Identify	Perform Periodic External Penetration Tests		•	•	Y	The frequency of testing can be difficult to determine, especially when multiple versions of an app can be pushed in a single day. This will be a decision decided by the organization in question.
18.3	Network	Protect	Remediate Penetration Test Findings		•	•	Y	Penetration testing results applicable to mobile systems should be remediated.
18.4	Network	Protect	Validate Security Measures			•	Y	Relevant EMM/MTD security measures should be used for implementing this safeguard, as applicable.
18.5		Identify	Perform Periodic Internal Penetration Tests			•	Y	Internal testing teams should review the security of mobile devices and supporting infrastructure on a regular basis.

5 GSMA Security Controls

5.1 GSMA Baseline Security Controls

Mobile Network Operators provide the backbone for mobile telecommunication technologies. At enterprise level the industry offers a wide array of diverse services ranging from traditional connectivity to content and managed services. The GSMA developed baseline security controls in its Official Document FS.31 [i.14] to help Operators understand and develop their security posture to a foundation (base) level. FS.31 [i.14] outlines a specific set of security controls that the mobile telecommunications industry should consider deploying. The solution descriptions identify specific advice that would allow the Operator to fulfil the control objectives. These controls stand separate to, but may be supported by, local market legislation and regulation. They do not replace or override local regulations or legislation in any territory. Their purpose is to enhance and supplement security levels within the mobile telecommunications industry. The controls include Network Function Virtualisation implementations.

The GSMA FS.31 Baseline Security Controls [i.14] are divided into several sub-sections and tables that are organized depending on the applicability of the types of GSMA Operator members and other stakeholders. Each table is organized into three columns:

- Reference: the unique reference for Baseline Security Control set.
- Objective: the objective that is to be achieved by implementation of each control set.
- Solution Description: the envisaged set of controls and standards applicable to each control objective.

The twenty control groups are shown in Table 5.1-1, below. The authoritative reference is found in FS.31 [i.14].

Table 5.1-1: GSMA Baseline Security Control set

Reference	Control Group
BC-001 - BC-015	Business Controls
SIM-001 - SIM-002	(e)UICC Management Controls
UE-001 - UE-003	User Equipment and Mobile Equipment Controls
IOT-001 - IOT-006	Internet of Things Controls
RN-001 - RN-006	Radio Network Operational Controls
ARCH-001 - ARCH-012	Network Architecture Controls
NFVI-VS-001 - NFVI-VS-010	Virtualisation Controls
NFVI-NS-001 - NFVI-NS-006	Network Controls
NFVI-SS-001 - NFVI-SS-003	Storage Controls
NFVI-MS-001 - NFVI-MS-002	Management Controls
CC-001 - CC-008	Container Controls
NS-001 - CC-011	Network Services Controls
CN-001 - CN-008	Core Network Management Controls
EC-001 - EC-007	Mobile Edge Computing Platform Controls
NEF-001 - NEF-008	Network Exposure Functions Controls
NO-001 - NO017	Network Operations Controls
VNF-LCM-001 - NFVI-LCM-004	VNF LCM Security Controls
VNFV-OR-001 - NFV-OR-004	Orchestrator Security Controls
SO-001 - SO-006	Security Operations Controls
RI-001 - RI-003	Roaming and Interconnect Controls

5.2 Critical Security Controls Mapping to GSMA Baseline Security Controls

Implementation of GSMA Baseline Security Controls can be accomplished using the Critical Security Controls [i.10] - which have been mapped in cooperation with GSMA [i.16]. The methodology used to create the mapping can be useful to anyone attempting to understand the relationships between the Critical Security Controls and GSMA FS.31 [i.14]. The overall goal for the mappings is to be as specific as possible, leaning towards under-mapping versus over-mapping. It is not enough for two Controls to be related; it should be clear that implementing one Control will contribute to implementing the other. The general strategy used is to identify all of the aspects within a Control and attempt to discern if both items state exactly the same thing. For instance:

- Safeguard 6.1: Establish an Access Granting Process.
- Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.

For a defensive mitigation to map to this Safeguard it should have at least one of the following:

- A clearly documented process, covering both new employees and changes in access.
- All relevant enterprise access control should be covered under this process, there can be no separation where different teams control access to different assets.
- Automated tools are ideally used, such as a SSO provider or routing access control through a directory service.
- The same process is followed every time a user's rights change, so a user never amasses greater rights access without documentation.

If the two concepts are effectively equal, they are mapped with the relationship "equivalent". If they are not equal but still related, the exact type of relationship between two defensive mitigations can be further explored. The relationships can be further analysed to understand how similar or different the two defensive mitigations are. The relationship column will contain one of four possible values:

- Equivalent: The defensive mitigation contains the exact same security concept as the Critical Security Control.
- Superset: The Control is partially or mostly related to the defensive mitigation in question, but the Control is a broader concept.
- Subset: The Safeguard is partially or mostly related, yet is still subsumed within the defensive mitigation. The defensive mitigation in question is a broader concept than the Control.
- No relationship: This will be represented by a blank cell.

The relationships should be read from left to right, like a sentence. Safeguard X is Equivalent to this < >.

EXAMPLES:

- Safeguard 16.8 "Separate Production and Non-Production Systems" is EQUIVALENT to NIST Cybersecurity Framework (CSF) Subcategory PR.DS-7 [i.22].
- Safeguard 3.5 "Securely Dispose of Data" is a SUBSET of NIST Cybersecurity Framework (CSF) Subcategory PR.DS-3 [i.22].

The Controls are written with certain principles in mind, such as only having one ask per Safeguard. This means many of the mapping targets are written in a way that contain multiple Safeguards within the same defensive mitigation, so the relationship can often be "Subset". Mappings are available from a variety of sources online, and different individuals may make their own decisions on the type of relationship.

A schematic of the detailed mapping [i.16] is provided below, together with a reverse mapping in Annex A.

Table 5.2-1

CSC Safeguard	Asset Type	Security Function	Title	IG1	IG2	IG3	GSMA FS.31 Control
Control 1: Inventory and Control of Enterprise Assets							
1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	X	X	X	NO-001
1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	X	X	X	NO-004
1.2	Devices	Respond	Address Unauthorized Assets	X	X	X	
1.3	Devices	Detect	Utilize an Active Discovery Tool		X	X	
1.4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		X	X	
1.5	Devices	Detect	Use a Passive Asset Discovery Tool			X	
Control 2: Inventory and Control of Software Assets							
2.1	Applications	Identify	Establish and Maintain a Software Inventory	X	X	X	
2.2	Applications	Identify	Ensure Authorized Software is Currently Supported	X	X	X	
2.3	Applications	Respond	Address Unauthorized Software	X	X	X	
2.4	Applications	Detect	Utilize Automated Software Inventory Tools		X	X	
2.5	Applications	Protect	Allowlist Authorized Software		X	X	CC-004
2.5	Applications	Protect	Allowlist Authorized Software		X	X	CC-005
2.5	Applications	Protect	Allowlist Authorized Software		X	X	EC-003
2.6	Applications	Protect	Allowlist Authorized Libraries		X	X	
2.7	Applications	Protect	Allowlist Authorized Scripts			X	NO-005
Control 3: Data Protection							
3.1	Data	Identify	Establish and Maintain a Data Management Process	X	X	X	BC-003
3.2	Data	Identify	Establish and Maintain a Data Inventory	X	X	X	
3.3	Data	Protect	Configure Data Access Control Lists	X	X	X	CN-008
3.3	Data	Protect	Configure Data Access Control Lists	X	X	X	NO-010
3.4	Data	Protect	Enforce Data Retention	X	X	X	
3.5	Data	Protect	Securely Dispose of Data	X	X	X	BC-12
3.5	Data	Protect	Securely Dispose of Data	X	X	X	CC-002
3.5	Data	Protect	Securely Dispose of Data	X	X	X	NFVI-SS-002
3.6	Devices	Protect	Encrypt Data on End-User Devices	X	X	X	
3.7	Data	Identify	Establish and Maintain a Data Classification Scheme		X	X	BC-003
3.8	Data	Identify	Document Data Flows		X	X	
3.9	Data	Protect	Encrypt Data on Removable Media		X	X	
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	RN-001
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	CN-002
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	NO-010
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	ARCH-006
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	ARCH-011
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	ARCH-008
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	NFVI-NS-002
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	NS-05
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	NS-003
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	EC-001
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	EC-005
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	NFV-OR-003
3.10	Data	Protect	Encrypt Sensitive Data in Transit		X	X	NFVI-VS-006
3.11	Data	Protect	Encrypt Sensitive Data at Rest		X	X	NO-010
3.11	Data	Protect	Encrypt Sensitive Data at Rest		X	X	NFVI-VS-002
3.11	Data	Protect	Encrypt Sensitive Data at Rest		X	X	NFVI-VS-007
3.11	Data	Protect	Encrypt Sensitive Data at Rest		X	X	NFVI-SS-001
3.11	Data	Protect	Encrypt Sensitive Data at Rest		X	X	NFVI-SS-003
3.11	Data	Protect	Encrypt Sensitive Data at Rest		X	X	CC-001
3.11	Data	Protect	Encrypt Sensitive Data at Rest		X	X	CC-002
3.11	Data	Protect	Encrypt Sensitive Data at Rest		X	X	NS-004
3.11	Data	Protect	Encrypt Sensitive Data at Rest		X	X	NS-009

CSC Safeguard	Asset Type	Security Function	Title	IG1	IG2	IG3	GSMA FS.31 Control
3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity		X	X	CN-008
3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity		X	X	EC-004
3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity		X	X	NO-003
3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity		X	X	ARCH-003
3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity		X	X	CC-003
3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity		X	X	CC-004
3.13	Data	Protect	Deploy a Data Loss Prevention Solution			X	CN-008
3.13	Data	Protect	Deploy a Data Loss Prevention Solution			X	NO-010
3.14	Data	Detect	Log Sensitive Data Access			X	CN-008
3.14	Data	Detect	Log Sensitive Data Access			X	NO-010
Control 4:Secure Configuration of Enterprise Assets and Software							
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	X	X	X	BC-003
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	X	X	X	NO-002
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	X	X	X	NO-017
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	X	X	X	NFVI-VS-001
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	X	X	X	NFVI-NS-006
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	X	X	X	CC-001
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	X	X	X	CC-003
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	X	X	X	NS-004
4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	X	X	X	NO-002
4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	X	X	X	NO-003
4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	X	X	X	NFVI-NS-001
4.3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets	X	X	X	
4.4	Devices	Protect	Implement and Manage a Firewall on Servers	X	X	X	CN-002
4.4	Devices	Protect	Implement and Manage a Firewall on Servers	X	X	X	NO-004
4.4	Devices	Protect	Implement and Manage a Firewall on Servers	X	X	X	EC-002
4.5	Devices	Protect	Implement and Manage a Firewall on End-User Devices	X	X	X	NO-004
4.5	Devices	Protect	Implement and Manage a Firewall on End-User Devices	X	X	X	EC-002
4.6	Network	Protect	Securely Manage Enterprise Assets and Software	X	X	X	
4.7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software	X	X	X	NO-001
4.7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software	X	X	X	NO-005
4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		X	X	CC-001

CSC Safeguard	Asset Type	Security Function	Title	IG1	IG2	IG3	GSMA FS.31 Control
4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		X	X	NFVI-VS-005
4.9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets		X	X	
4.10	Devices	Respond	Enforce Automatic Device Lockout on Portable End-User Devices		X	X	
4.11	Devices	Protect	Enforce Remote Wipe Capability on Portable End-User Devices		X	X	
4.12	Devices	Protect	Separate Enterprise Workspaces on Mobile End-User Devices			X	
Control 5: Account Management							
5.1	Users	Identify	Establish and Maintain an Inventory of Accounts	X	X	X	NO-005
5.2	Users	Protect	Use Unique Passwords	X	X	X	NFVI-MS-001
5.2	Users	Protect	Use Unique Passwords	X	X	X	NO-005
5.3	Users	Respond	Disable Dormant Accounts	X	X	X	CN-008
5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	X	X	X	NO-005
5.5	Users	Identify	Establish and Maintain an Inventory of Service Accounts		X	X	
5.6	Users	Protect	Centralize Account Management		X	X	
Control 6: Access Control Management							
6.1	Users	Protect	Establish an Access Granting Process	X	X	X	CN-001
6.2	Users	Protect	Establish an Access Revoking Process	X	X	X	CN-001
6.3	Users	Protect	Require MFA for Externally-Exposed Applications	X	X	X	
6.4	Users	Protect	Require MFA for Remote Network Access	X	X	X	
6.5	Users	Protect	Require MFA for Administrative Access	X	X	X	NO-005
6.6	Users	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems		X	X	
6.7	Users	Protect	Centralize Access Control		X	X	NS-001
6.8	Data	Protect	Define and Maintain Role-Based Access Control			X	BC-003
6.8	Data	Protect	Define and Maintain Role-Based Access Control			X	NFVI-MS-001
6.8	Data	Protect	Define and Maintain Role-Based Access Control			X	CC-004
6.8	Data	Protect	Define and Maintain Role-Based Access Control			X	CN-008
Control 7: Continuous Vulnerability Management							
7.1	Applications	Protect	Establish and Maintain a Vulnerability Management Process	X	X	X	BC-003
7.1	Applications	Protect	Establish and Maintain a Vulnerability Management Process	X	X	X	NO-006
7.2	Applications	Respond	Establish and Maintain a Remediation Process	X	X	X	BC-004
7.2	Applications	Respond	Establish and Maintain a Remediation Process	X	X	X	NO-006
7.2	Applications	Respond	Establish and Maintain a Remediation Process	X	X	X	NO-016
7.3	Applications	Protect	Perform Automated Operating System Patch Management	X	X	X	UE-002
7.3	Applications	Protect	Perform Automated Operating System Patch Management	X	X	X	NO-016
7.3	Applications	Protect	Perform Automated Operating System Patch Management	X	X	X	NFVI-VS-005
7.4	Applications	Protect	Perform Automated Application Patch Management	X	X	X	UE-002
7.4	Applications	Protect	Perform Automated Application Patch Management	X	X	X	NO-016
7.4	Applications	Protect	Perform Automated Application Patch Management	X	X	X	CC-007

CSC Safeguard	Asset Type	Security Function	Title	IG1	IG2	IG3	GSMA FS.31 Control
7.4	Applications	Protect	Perform Automated Application Patch Management	X	X	X	NFVI-VS-005
7.5	Applications	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets		X	X	NO-006
7.5	Applications	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets		X	X	CC-005
7.5	Applications	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets		X	X	SO-005
7.6	Applications	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		X	X	NO-004
7.6	Applications	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		X	X	NO-006
7.6	Applications	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		X	X	SO-005
7.7	Applications	Respond	Remediate Detected Vulnerabilities		X	X	NO-006
7.7	Applications	Respond	Remediate Detected Vulnerabilities		X	X	SO-005
Control 8: Audit Log Management							
8.1	Network	Protect	Establish and Maintain an Audit Log Management Process	X	X	X	BC-003
8.1	Network	Protect	Establish and Maintain an Audit Log Management Process	X	X	X	BC-004
8.1	Network	Protect	Establish and Maintain an Audit Log Management Process	X	X	X	NO-007
8.1	Network	Protect	Establish and Maintain an Audit Log Management Process	X	X	X	SO-001
8.1	Network	Protect	Establish and Maintain an Audit Log Management Process	X	X	X	SO-006
8.2	Network	Detect	Collect Audit Logs	X	X	X	RI-004
8.2	Network	Detect	Collect Audit Logs	X	X	X	NS-006
8.2	Network	Detect	Collect Audit Logs	X	X	X	NO-007
8.2	Network	Detect	Collect Audit Logs	X	X	X	NO-015
8.2	Network	Detect	Collect Audit Logs	X	X	X	SO-001
8.2	Network	Detect	Collect Audit Logs	X	X	X	SO-006
8.3	Network	Protect	Ensure Adequate Audit Log Storage	X	X	X	
8.4	Network	Protect	Standardize Time Synchronization		X	X	NFVI-VS-009
8.5	Network	Detect	Collect Detailed Audit Logs		X	X	CC-007
8.5	Network	Detect	Collect Detailed Audit Logs		X	X	NO-005
8.5	Network	Detect	Collect Detailed Audit Logs		X	X	NO-010
8.6	Network	Detect	Collect DNS Query Audit Logs		X	X	
8.7	Network	Detect	Collect URL Request Audit Logs		X	X	
8.8	Devices	Detect	Collect Command-Line Audit Logs		X	X	
8.9	Network	Detect	Centralize Audit Logs		X	X	SO-006
8.10	Network	Protect	Retain Audit Logs		X	X	
8.11	Network	Detect	Conduct Audit Log Reviews		X	X	BC-004
8.11	Network	Detect	Conduct Audit Log Reviews		X	X	NO-007
8.11	Network	Detect	Conduct Audit Log Reviews		X	X	NO-015
8.11	Network	Detect	Conduct Audit Log Reviews		X	X	SO-001
8.11	Network	Detect	Conduct Audit Log Reviews		X	X	SO-006
8.12	Data	Detect	Collect Service Provider Logs			X	
Control 9: Email and Web Browser Protections							
9.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	X	X	X	
9.2	Network	Protect	Use DNS Filtering Services	X	X	X	
9.3	Network	Protect	Maintain and Enforce Network-Based URL Filters		X	X	
9.4	Applications	Protect	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		X	X	
9.5	Network	Protect	Implement DMARC		X	X	
9.6	Network	Protect	Block Unnecessary File Types		X	X	
9.7	Network	Protect	Deploy and Maintain Email Server Anti-Malware Protections			X	SO-002
Control 10: Malware Defenses							
10.1	Devices	Protect	Deploy and Maintain Anti-Malware Software	X	X	X	SO-002

CSC Safeguard	Asset Type	Security Function	Title	IG1	IG2	IG3	GSMA FS.31 Control
10.1	Devices	Protect	Deploy and Maintain Anti-Malware Software	X	X	X	CC-005
10.2	Devices	Protect	Configure Automatic Anti-Malware Signature Updates	X	X	X	SO-002
10.2	Devices	Protect	Configure Automatic Anti-Malware Signature Updates	X	X	X	NFVI-VS-002
10.3	Devices	Protect	Disable Autorun and Autoplay for Removable Media	X	X	X	
10.4	Devices	Detect	Configure Automatic Anti-Malware Scanning of Removable Media		X	X	
10.5	Devices	Protect	Enable Anti-Exploitation Features		X	X	CC-005
10.5	Devices	Protect	Enable Anti-Exploitation Features		X	X	NFVI-VS-004
10.6	Devices	Protect	Centrally Manage Anti-Malware Software		X	X	SO-002
10.7	Devices	Detect	Use behaviour-Based Anti-Malware Software		X	X	
Control 11: Data Recovery							
11.1	Data	Recover	Establish and Maintain a Data Recovery Process	X	X	X	BC-003
11.1	Data	Recover	Establish and Maintain a Data Recovery Process	X	X	X	BC-008
11.2	Data	Recover	Perform Automated Backups	X	X	X	
11.3	Data	Protect	Protect Recovery Data	X	X	X	NFVI-VS-007
11.4	Data	Recover	Establish and Maintain an Isolated Instance of Recovery Data	X	X	X	
11.5	Data	Recover	Test Data Recovery		X	X	SO-004
Control 12: Network Infrastructure Management							
12.1	Network	Protect	Ensure Network Infrastructure is Up-to-Date	X	X	X	NO-016
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	BC-003
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	BC-004
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	RN-007
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	RI-002
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	ARCH-003
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	ARCH-004
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	ARCH-005
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	ARCH-007
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	ARCH-012
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	NFVI-NS-002
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	NFVI-NS-003
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		X	X	NFVI-NS-006
12.3	Network	Protect	Securely Manage Network Infrastructure		X	X	RN-006
12.3	Network	Protect	Securely Manage Network Infrastructure		X	X	RN-007
12.3	Network	Protect	Securely Manage Network Infrastructure		X	X	ARCH-006
12.3	Network	Protect	Securely Manage Network Infrastructure		X	X	NFVI-VS-001
12.3	Network	Protect	Securely Manage Network Infrastructure		X	X	NFVI-NS-002
12.3	Network	Protect	Securely Manage Network Infrastructure		X	X	CC-001
12.3	Network	Protect	Securely Manage Network Infrastructure		X	X	NS-05
12.4	Network	Identify	Establish and Maintain Architecture Diagram(s)		X	X	
12.5	Network	Protect	Centralize Network Authentication, Authorization, and Auditing (AAA)		X	X	
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		X	X	ARCH-006

CSC Safeguard	Asset Type	Security Function	Title	IG1	IG2	IG3	GSMA FS.31 Control
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		X	X	ARCH-006
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		X	X	CC-002
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		X	X	CC-007
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		X	X	CC-008
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		X	X	NS-003
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		X	X	NS-005
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		X	X	NFV-OR-002
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		X	X	NFVI-VS-006
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		X	X	NFVI-NS-004
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		X	X	NEF-002
12.7	Devices	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		X	X	
Control 13: Network Monitoring and Defense							
13.1	Network	Detect	Centralize Security Event Alerting		X	X	RI-004
13.1	Network	Detect	Centralize Security Event Alerting		X	X	NS-009
13.1	Network	Detect	Centralize Security Event Alerting		X	X	NO-007
13.1	Network	Detect	Centralize Security Event Alerting		X	X	NO-012
13.1	Network	Detect	Centralize Security Event Alerting		X	X	NO-013
13.1	Network	Detect	Centralize Security Event Alerting		X	X	SO-001
13.1	Network	Detect	Centralize Security Event Alerting		X	X	SO-006
13.1	Network	Detect	Centralize Security Event Alerting		X	X	EC-007
13.2	Devices	Detect	Deploy a Host-Based Intrusion Detection Solution		X	X	
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution		X	X	RN-003
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution		X	X	CC-007
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution		X	X	NO-012
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution		X	X	NO-013
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution		X	X	NO-015
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution		X	X	EC-007
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments		X	X	RI-001
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments		X	X	ARCH-002
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments		X	X	ARCH-004
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments		X	X	ARCH-011
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments		X	X	CC-003
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments		X	X	CC-007
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments		X	X	EC-002
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments		X	X	NS-09
13.5	Devices	Protect	Manage Access Control for Remote Assets		X	X	
13.6	Network	Detect	Collect Network Traffic Flow Logs		X	X	CC-007

CSC Safeguard	Asset Type	Security Function	Title	IG1	IG2	IG3	GSMA FS.31 Control
13.6	Network	Detect	Collect Network Traffic Flow Logs		X	X	NO-014
13.6	Network	Detect	Collect Network Traffic Flow Logs		X	X	SO-001
13.7	Devices	Protect	Deploy a Host-Based Intrusion Prevention Solution			X	
13.8	Network	Protect	Deploy a Network Intrusion Prevention Solution			X	NO-013
13.9	Devices	Protect	Deploy Port-Level Access Control			X	ARCH-010
13.9	Devices	Protect	Deploy Port-Level Access Control			X	NO-001
13.9	Devices	Protect	Deploy Port-Level Access Control			X	NO-004
13.10	Network	Protect	Perform Application Layer Filtering			X	RI-001
13.10	Network	Protect	Perform Application Layer Filtering			X	NO-004
13.10	Network	Protect	Perform Application Layer Filtering			X	NS-009
13.11	Network	Detect	Tune Security Event Alerting Thresholds			X	NO-007
13.11	Network	Detect	Tune Security Event Alerting Thresholds			X	SO-006
Control 14: Security Awareness and Skills Training							
14.1	N/A	Protect	Establish and Maintain a Security Awareness Program	X	X	X	BC-003
14.2	N/A	Protect	Train Workforce Members to Recognize Social Engineering Attacks	X	X	X	
14.3	N/A	Protect	Train Workforce Members on Authentication Best Practices	X	X	X	
14.4	N/A	Protect	Train Workforce on Data Handling Best Practices	X	X	X	
14.5	N/A	Protect	Train Workforce Members on Causes of Unintentional Data Exposure	X	X	X	
14.6	N/A	Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	X	X	X	
14.7	N/A	Protect	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	X	X	X	
14.8	N/A	Protect	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	X	X	X	
14.9	N/A	Protect	Conduct Role-Specific Security Awareness and Skills Training		X	X	
Control 15: Service Provider Management							
15.1	N/A	Identify	Establish and Maintain an Inventory of Service Providers	X	X	X	
15.2	N/A	Identify	Establish and Maintain a Service Provider Management Policy		X	X	BC-003
15.2	N/A	Identify	Establish and Maintain a Service Provider Management Policy		X	X	SIM-001
15.3	N/A	Identify	Classify Service Providers		X	X	
15.4	N/A	Protect	Ensure Service Provider Contracts Include Security Requirements		X	X	BC-010
15.4	N/A	Protect	Ensure Service Provider Contracts Include Security Requirements		X	X	SIM-002
15.4	N/A	Protect	Ensure Service Provider Contracts Include Security Requirements		X	X	IOT-001
15.4	N/A	Protect	Ensure Service Provider Contracts Include Security Requirements		X	X	IOT-002
15.4	N/A	Protect	Ensure Service Provider Contracts Include Security Requirements		X	X	IOT-003
15.4	N/A	Protect	Ensure Service Provider Contracts Include Security Requirements		X	X	IOT-004
15.4	N/A	Protect	Ensure Service Provider Contracts Include Security Requirements		X	X	IOT-006
15.4	N/A	Protect	Ensure Service Provider Contracts Include Security Requirements		X	X	NO-011
15.5	N/A	Identify	Assess Service Providers			X	BC-11
15.5	N/A	Identify	Assess Service Providers			X	IOT-001
15.5	N/A	Identify	Assess Service Providers			X	IOT-002
15.5	N/A	Identify	Assess Service Providers			X	IOT-003
15.5	N/A	Identify	Assess Service Providers			X	IOT-004

CSC Safeguard	Asset Type	Security Function	Title	IG1	IG2	IG3	GSMA FS.31 Control
15.5	N/A	Identify	Assess Service Providers			X	IOT-005
15.6	Data	Detect	Monitor Service Providers			X	
15.7	Data	Protect	Securely Decommission Service Providers			X	
Control 16: Application Software Security							
16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process		X	X	BC-003
16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process		X	X	BC-004
16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process		X	X	BC-005
16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process		X	X	BC-006
16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process		X	X	BC-007
16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process		X	X	NEF-006
16.2	Applications	Protect	Establish and Maintain a Process to Accept and Address Software Vulnerabilities		X	X	
16.3	Applications	Protect	Perform Root Cause Analysis on Security Vulnerabilities		X	X	
16.4	Applications	Protect	Establish and Manage an Inventory of Third-Party Software Components		X	X	
16.5	Applications	Protect	Use Up-to-Date and Trusted Third-Party Software Components		X	X	
16.6	Applications	Protect	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities		X	X	BC-005
16.6	Applications	Protect	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities		X	X	NO-006
16.7	Applications	Protect	Use Standard Hardening Configuration Templates for Application Infrastructure		X	X	
16.8	Applications	Protect	Separate Production and Non-Production Systems		X	X	
16.9	Applications	Protect	Train Developers in Application Security Concepts and Secure Coding		X	X	
16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures		X	X	BC-005
16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures		X	X	NO-005
16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures		X	X	CC-008
16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures		X	X	NS-006
16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures		X	X	NFVI-MS-002
16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures		X	X	EC-005
16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures		X	X	NEF-006
16.11	Applications	Protect	Leverage Vetted Modules or Services for Application Security Components		X	X	
16.12	Applications	Protect	Implement Code-Level Security Checks			X	BC-004
16.13	Applications	Protect	Conduct Application Penetration Testing			X	
16.14	Applications	Protect	Conduct Threat Modelling			X	
Control 17: Incident Response Management							
17.1	N/A	Respond	Designate Personnel to Manage Incident Handling	X	X	X	SO-004
17.2	N/A	Respond	Establish and Maintain Contact Information for Reporting Security Incidents	X	X	X	SO-004
17.3	N/A	Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	X	X	X	BC-004

CSC Safeguard	Asset Type	Security Function	Title	IG1	IG2	IG3	GSMA FS.31 Control
17.3	N/A	Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	X	X	X	SO-004
17.4	N/A	Respond	Establish and Maintain an Incident Response Process		X	X	BC-003
17.4	N/A	Respond	Establish and Maintain an Incident Response Process		X	X	BC-008
17.4	N/A	Respond	Establish and Maintain an Incident Response Process		X	X	SO-004
17.5	N/A	Respond	Assign Key Roles and Responsibilities		X	X	SO-004
17.6	N/A	Respond	Define Mechanisms for Communicating During Incident Response		X	X	SO-004
17.7	N/A	Recover	Conduct Routine Incident Response Exercises		X	X	SO-004
17.8	N/A	Recover	Conduct Post-Incident Reviews		X	X	SO-004
17.9	N/A	Recover	Establish and Maintain Security Incident Thresholds			X	BC-004
Control 18: Penetration Testing							
18.1	N/A	Identify	Establish and Maintain a Penetration Testing Program		X	X	SO-005
18.2	Network	Identify	Perform Periodic External Penetration Tests		X	X	SO-005
18.3	Network	Protect	Remediate Penetration Test Findings		X	X	SO-005
18.4	Network	Protect	Validate Security Measures			X	
18.5	N/A	Identify	Perform Periodic Internal Penetration Tests			X	SO-005

Annex A: Reverse Mapping of GSMA FS.31 Controls to ETSI Critical Security Controls

GSMA FS.31 Control	CSC Safeguard	Title
ARCH-002	13.4	Perform Traffic Filtering Between Network Segments
ARCH-003	3.12	Segment Data Processing and Storage Based on Sensitivity
ARCH-003	12.2	Establish and Maintain a Secure Network Architecture
ARCH-004	12.2	Establish and Maintain a Secure Network Architecture
ARCH-004	13.4	Perform Traffic Filtering Between Network Segments
ARCH-005	12.2	Establish and Maintain a Secure Network Architecture
ARCH-006	3.10	Encrypt Sensitive Data in Transit
ARCH-006	12.3	Securely Manage Network Infrastructure
ARCH-006	12.6	Use of Secure Network Management and Communication Protocols
ARCH-006	12.6	Use of Secure Network Management and Communication Protocols
ARCH-007	12.2	Establish and Maintain a Secure Network Architecture
ARCH-008	3.10	Encrypt Sensitive Data in Transit
ARCH-010	13.9	Deploy Port-Level Access Control
ARCH-011	3.10	Encrypt Sensitive Data in Transit
ARCH-011	13.4	Perform Traffic Filtering Between Network Segments
ARCH-012	12.2	Establish and Maintain a Secure Network Architecture
BC-003	3.1	Establish and Maintain a Data Management Process
BC-003	3.7	Establish and Maintain a Data Classification Scheme
BC-003	4.1	Establish and Maintain a Secure Configuration Process
BC-003	6.8	Define and Maintain Role-Based Access Control
BC-003	7.1	Establish and Maintain a Vulnerability Management Process
BC-003	8.1	Establish and Maintain an Audit Log Management Process
BC-003	11.1	Establish and Maintain a Data Recovery Process
BC-003	12.2	Establish and Maintain a Secure Network Architecture
BC-003	14.1	Establish and Maintain a Security Awareness Program
BC-003	15.2	Establish and Maintain a Service Provider Management Policy
BC-003	16.1	Establish and Maintain a Secure Application Development Process
BC-003	17.4	Establish and Maintain an Incident Response Process
BC-004	7.2	Establish and Maintain a Remediation Process
BC-004	8.1	Establish and Maintain an Audit Log Management Process
BC-004	8.11	Conduct Audit Log Reviews
BC-004	12.2	Establish and Maintain a Secure Network Architecture
BC-004	16.1	Establish and Maintain a Secure Application Development Process
BC-004	16.12	Implement Code-Level Security Checks
BC-004	17.3	Establish and Maintain an Enterprise Process for Reporting Incidents
BC-004	17.9	Establish and Maintain Security Incident Thresholds
BC-005	16.1	Establish and Maintain a Secure Application Development Process
BC-005	16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities
BC-005	16.10	Apply Secure Design Principles in Application Architectures
BC-006	16.1	Establish and Maintain a Secure Application Development Process
BC-007	16.1	Establish and Maintain a Secure Application Development Process
BC-008	11.1	Establish and Maintain a Data Recovery Process
BC-008	17.4	Establish and Maintain an Incident Response Process
BC-010	15.4	Ensure Service Provider Contracts Include Security Requirements
BC-11	15.5	Assess Service Providers
BC-12	3.5	Securely Dispose of Data
CC-001	3.11	Encrypt Sensitive Data at Rest
CC-001	4.1	Establish and Maintain a Secure Configuration Process
CC-001	4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
CC-001	12.3	Securely Manage Network Infrastructure
CC-002	3.5	Securely Dispose of Data
CC-002	3.11	Encrypt Sensitive Data at Rest
CC-002	12.6	Use of Secure Network Management and Communication Protocols
CC-003	3.12	Segment Data Processing and Storage Based on Sensitivity

GSMA FS.31 Control	CSC Safeguard	Title
CC-003	4.1	Establish and Maintain a Secure Configuration Process
CC-003	13.4	Perform Traffic Filtering Between Network Segments
CC-004	2.5	Allowlist Authorized Software
CC-004	3.12	Segment Data Processing and Storage Based on Sensitivity
CC-004	6.8	Define and Maintain Role-Based Access Control
CC-005	2.5	Allowlist Authorized Software
CC-005	7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets
CC-005	10.1	Deploy and Maintain Anti-Malware Software
CC-005	10.5	Enable Anti-Exploitation Features
CC-007	7.4	Perform Automated Application Patch Management
CC-007	8.5	Collect Detailed Audit Logs
CC-007	12.6	Use of Secure Network Management and Communication Protocols
CC-007	13.3	Deploy a Network Intrusion Detection Solution
CC-007	13.4	Perform Traffic Filtering Between Network Segments
CC-007	13.6	Collect Network Traffic Flow Logs
CC-008	12.6	Use of Secure Network Management and Communication Protocols
CC-008	16.10	Apply Secure Design Principles in Application Architectures
CN-001	6.1	Establish an Access Granting Process
CN-001	6.2	Establish an Access Revoking Process
CN-002	3.10	Encrypt Sensitive Data in Transit
CN-002	4.4	Implement and Manage a Firewall on Servers
CN-008	3.3	Configure Data Access Control Lists
CN-008	3.12	Segment Data Processing and Storage Based on Sensitivity
CN-008	3.13	Deploy a Data Loss Prevention Solution
CN-008	3.14	Log Sensitive Data Access
CN-008	5.3	Disable Dormant Accounts
CN-008	6.8	Define and Maintain Role-Based Access Control
EC-001	3.10	Encrypt Sensitive Data in Transit
EC-002	4.4	Implement and Manage a Firewall on Servers
EC-002	4.5	Implement and Manage a Firewall on End-User Devices
EC-002	13.4	Perform Traffic Filtering Between Network Segments
EC-003	2.5	Allowlist Authorized Software
EC-004	3.12	Segment Data Processing and Storage Based on Sensitivity
EC-005	3.10	Encrypt Sensitive Data in Transit
EC-005	16.10	Apply Secure Design Principles in Application Architectures
EC-007	13.1	Centralize Security Event Alerting
EC-007	13.3	Deploy a Network Intrusion Detection Solution
IOT-001	15.4	Ensure Service Provider Contracts Include Security Requirements
IOT-001	15.5	Assess Service Providers
IOT-002	15.4	Ensure Service Provider Contracts Include Security Requirements
IOT-002	15.5	Assess Service Providers
IOT-003	15.4	Ensure Service Provider Contracts Include Security Requirements
IOT-003	15.5	Assess Service Providers
IOT-004	15.4	Ensure Service Provider Contracts Include Security Requirements
IOT-004	15.5	Assess Service Providers
IOT-005	15.5	Assess Service Providers
IOT-006	15.4	Ensure Service Provider Contracts Include Security Requirements
NEF-002	12.6	Use of Secure Network Management and Communication Protocols
NEF-006	16.1	Establish and Maintain a Secure Application Development Process
NEF-006	16.10	Apply Secure Design Principles in Application Architectures
NFVI-MS-001	5.2	Use Unique Passwords
NFVI-MS-001	6.8	Define and Maintain Role-Based Access Control
NFVI-MS-002	16.10	Apply Secure Design Principles in Application Architectures
NFVI-NS-001	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure
NFVI-NS-002	3.10	Encrypt Sensitive Data in Transit
NFVI-NS-002	12.2	Establish and Maintain a Secure Network Architecture
NFVI-NS-002	12.3	Securely Manage Network Infrastructure
NFVI-NS-003	12.2	Establish and Maintain a Secure Network Architecture
NFVI-NS-004	12.6	Use of Secure Network Management and Communication Protocols
NFVI-NS-006	4.1	Establish and Maintain a Secure Configuration Process
NFVI-NS-006	12.2	Establish and Maintain a Secure Network Architecture
NFVI-SS-001	3.11	Encrypt Sensitive Data at Rest

GSMA FS.31 Control	CSC Safeguard	Title
NFVI-SS-002	3.5	Securely Dispose of Data
NFVI-SS-003	3.11	Encrypt Sensitive Data at Rest
NFVI-VS-001	4.1	Establish and Maintain a Secure Configuration Process
NFVI-VS-001	12.3	Securely Manage Network Infrastructure
NFVI-VS-002	3.11	Encrypt Sensitive Data at Rest
NFVI-VS-002	10.2	Configure Automatic Anti-Malware Signature Updates
NFVI-VS-004	10.5	Enable Anti-Exploitation Features
NFVI-VS-005	4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
NFVI-VS-005	7.3	Perform Automated Operating System Patch Management
NFVI-VS-005	7.4	Perform Automated Application Patch Management
NFVI-VS-006	3.10	Encrypt Sensitive Data in Transit
NFVI-VS-006	12.6	Use of Secure Network Management and Communication Protocols
NFVI-VS-007	3.11	Encrypt Sensitive Data at Rest
NFVI-VS-007	11.3	Protect Recovery Data
NFVI-VS-009	8.4	Standardize Time Synchronization
NFV-OR-002	12.6	Use of Secure Network Management and Communication Protocols
NFV-OR-003	3.10	Encrypt Sensitive Data in Transit
NO-001	1.1	Establish and Maintain Detailed Enterprise Asset Inventory
NO-001	4.7	Manage Default Accounts on Enterprise Assets and Software
NO-001	13.9	Deploy Port-Level Access Control
NO-002	4.1	Establish and Maintain a Secure Configuration Process
NO-002	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure
NO-003	3.12	Segment Data Processing and Storage Based on Sensitivity
NO-003	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure
NO-004	1.1	Establish and Maintain Detailed Enterprise Asset Inventory
NO-004	4.4	Implement and Manage a Firewall on Servers
NO-004	4.5	Implement and Manage a Firewall on End-User Devices
NO-004	7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
NO-004	13.9	Deploy Port-Level Access Control
NO-004	13.10	Perform Application Layer Filtering
NO-005	2.7	Allowlist Authorized Scripts
NO-005	4.7	Manage Default Accounts on Enterprise Assets and Software
NO-005	5.1	Establish and Maintain an Inventory of Accounts
NO-005	5.2	Use Unique Passwords
NO-005	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts
NO-005	6.5	Require MFA for Administrative Access
NO-005	8.5	Collect Detailed Audit Logs
NO-005	16.10	Apply Secure Design Principles in Application Architectures
NO-006	7.1	Establish and Maintain a Vulnerability Management Process
NO-006	7.2	Establish and Maintain a Remediation Process
NO-006	7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets
NO-006	7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
NO-006	7.7	Remediate Detected Vulnerabilities
NO-006	16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities
NO-007	8.1	Establish and Maintain an Audit Log Management Process
NO-007	8.2	Collect Audit Logs
NO-007	8.11	Conduct Audit Log Reviews
NO-007	13.1	Centralize Security Event Alerting
NO-007	13.11	Tune Security Event Alerting Thresholds
NO-010	3.3	Configure Data Access Control Lists
NO-010	3.10	Encrypt Sensitive Data in Transit
NO-010	3.11	Encrypt Sensitive Data at Rest
NO-010	3.13	Deploy a Data Loss Prevention Solution
NO-010	3.14	Log Sensitive Data Access
NO-010	8.5	Collect Detailed Audit Logs
NO-011	15.4	Ensure Service Provider Contracts Include Security Requirements
NO-012	13.1	Centralize Security Event Alerting
NO-012	13.3	Deploy a Network Intrusion Detection Solution

GSMA FS.31 Control	CSC Safeguard	Title
NO-013	13.1	Centralize Security Event Alerting
NO-013	13.3	Deploy a Network Intrusion Detection Solution
NO-013	13.8	Deploy a Network Intrusion Prevention Solution
NO-014	13.6	Collect Network Traffic Flow Logs
NO-015	8.2	Collect Audit Logs
NO-015	8.11	Conduct Audit Log Reviews
NO-015	13.3	Deploy a Network Intrusion Detection Solution
NO-016	7.2	Establish and Maintain a Remediation Process
NO-016	7.3	Perform Automated Operating System Patch Management
NO-016	7.4	Perform Automated Application Patch Management
NO-016	12.1	Ensure Network Infrastructure is Up-to-Date
NO-017	4.1	Establish and Maintain a Secure Configuration Process
NS-001	6.7	Centralize Access Control
NS-003	3.10	Encrypt Sensitive Data in Transit
NS-003	12.6	Use of Secure Network Management and Communication Protocols
NS-004	3.11	Encrypt Sensitive Data at Rest
NS-004	4.1	Establish and Maintain a Secure Configuration Process
NS-005	12.6	Use of Secure Network Management and Communication Protocols
NS-006	8.2	Collect Audit Logs
NS-006	16.10	Apply Secure Design Principles in Application Architectures
NS-009	3.11	Encrypt Sensitive Data at Rest
NS-009	13.1	Centralize Security Event Alerting
NS-009	13.10	Perform Application Layer Filtering
NS-05	3.10	Encrypt Sensitive Data in Transit
NS-05	12.3	Securely Manage Network Infrastructure
NS-09	13.4	Perform Traffic Filtering Between Network Segments
RI-001	13.4	Perform Traffic Filtering Between Network Segments
RI-001	13.10	Perform Application Layer Filtering
RI-002	12.2	Establish and Maintain a Secure Network Architecture
RI-004	8.2	Collect Audit Logs
RI-004	13.1	Centralize Security Event Alerting
RN-001	3.10	Encrypt Sensitive Data in Transit
RN-003	13.3	Deploy a Network Intrusion Detection Solution
RN-006	12.3	Securely Manage Network Infrastructure
RN-007	12.2	Establish and Maintain a Secure Network Architecture
RN-007	12.3	Securely Manage Network Infrastructure
SIM-001	15.2	Establish and Maintain a Service Provider Management Policy
SIM-002	15.4	Ensure Service Provider Contracts Include Security Requirements
SO-001	8.1	Establish and Maintain an Audit Log Management Process
SO-001	8.2	Collect Audit Logs
SO-001	8.11	Conduct Audit Log Reviews
SO-001	13.1	Centralize Security Event Alerting
SO-001	13.6	Collect Network Traffic Flow Logs
SO-002	9.7	Deploy and Maintain Email Server Anti-Malware Protections
SO-002	10.1	Deploy and Maintain Anti-Malware Software
SO-002	10.2	Configure Automatic Anti-Malware Signature Updates
SO-002	10.6	Centrally Manage Anti-Malware Software
SO-004	11.5	Test Data Recovery
SO-004	17.1	Designate Personnel to Manage Incident Handling
SO-004	17.2	Establish and Maintain Contact Information for Reporting Security Incidents
SO-004	17.3	Establish and Maintain an Enterprise Process for Reporting Incidents
SO-004	17.4	Establish and Maintain an Incident Response Process
SO-004	17.5	Assign Key Roles and Responsibilities
SO-004	17.6	Define Mechanisms for Communicating During Incident Response
SO-004	17.7	Conduct Routine Incident Response Exercises
SO-004	17.8	Conduct Post-Incident Reviews
SO-005	7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets
SO-005	7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
SO-005	7.7	Remediate Detected Vulnerabilities
SO-005	18.1	Establish and Maintain a Penetration Testing Program
SO-005	18.2	Perform Periodic External Penetration Tests
SO-005	18.3	Remediate Penetration Test Findings

GSMA FS.31 Control	CSC Safeguard	Title
SO-005	18.5	Perform Periodic Internal Penetration Tests
SO-006	8.1	Establish and Maintain an Audit Log Management Process
SO-006	8.2	Collect Audit Logs
SO-006	8.9	Centralize Audit Logs
SO-006	8.11	Conduct Audit Log Reviews
SO-006	13.1	Centralize Security Event Alerting
SO-006	13.11	Tune Security Event Alerting Thresholds
UE-002	7.3	Perform Automated Operating System Patch Management
UE-002	7.4	Perform Automated Application Patch Management

Annex B: Bibliography

- Apple®: "[Use Automated Device Enrollment](#)".
- Apple: "[Introduction to Secure Coding](#)".
- Apple: "[Apple Platform Security](#)".
- Apple: "[Managing Devices and Corporate Data](#)".
- Apple: "[Apple Configurator Help, Prepare Devices](#)".
- American Chemistry Council: "[Cybersecurity](#)".
- CISA: "[Industrial Control Systems](#)".
- Google®: "[Application Signing](#)".
- Google: "[Android mobility best practice advisory](#)".
- Google: "[Android Security 2017 Year In Review](#)".
- Kotlin: "[Coding Conventions](#)".
- Google: "[Enterprise Solutions Directory](#)".
- ICS-ISAC: "[Blog](#)".
- MITRE, ATT&CK®: "[Mobile Tactics](#)".
- NIAP: "[Product Compliance List](#)".
- NIAP: "[Protection Profile for Application Software](#)".
- NIAP: "[Requirements for Vetting Mobile Apps from the Protection Profile for Application Software](#)".
- [NIST SP 800-101](#): "Guidelines on Mobile Device Forensics".
- NIST: "[Mobile Threat Catalogue](#)".
- Now Secure: "[Mobile App Security Testing Checklist](#)".
- Now Secure: "[Secure Mobile Development Best Practices](#)".
- Open Web Application Security Project (OWASP): "[Mobile Application Security](#)".
- Open Web Application Security Project (OWASP): "[Mobile Application Security Testing Guide](#)".
- Open Web Application Security Project (OWASP): "[Mobile Application Security Verification Standard \(MASVS\)](#)".
- Open Web Application Security Project (OWASP): "[Mobile Top 10](#)".
- SANS Institute: "[Cybersecurity Training Overview](#)".

History

Document history		
V1.1.1	July 2024	Publication